



---

Theses and Dissertations


---

2005-07-11

## Establishing Public Confidence in the Viability of Fingerprint Biometric Technology

Nathan Alan Green  
*Brigham Young University - Provo*

Follow this and additional works at: <https://scholarsarchive.byu.edu/etd>

 Part of the [Computer Sciences Commons](#), and the [Construction Engineering and Management Commons](#)

---

### BYU ScholarsArchive Citation

Green, Nathan Alan, "Establishing Public Confidence in the Viability of Fingerprint Biometric Technology" (2005). *Theses and Dissertations*. 586.  
<https://scholarsarchive.byu.edu/etd/586>

This Thesis is brought to you for free and open access by BYU ScholarsArchive. It has been accepted for inclusion in Theses and Dissertations by an authorized administrator of BYU ScholarsArchive. For more information, please contact [scholarsarchive@byu.edu](mailto:scholarsarchive@byu.edu), [ellen\\_amatangelo@byu.edu](mailto:ellen_amatangelo@byu.edu).

ESTABLISHING PUBLIC CONFIDENCE IN THE VIABILITY OF  
FINGERPRINT BIOMETRIC TECHNOLOGY

by

Nathan A. Green

A thesis submitted to the faculty of

Brigham Young University

in partial fulfillment of the requirements for the degree of

Master of Science

School of Technology

Brigham Young University

August 2005



BRIGHAM YOUNG UNIVERSITY

GRADUATE COMMITTEE APPROVAL

of a thesis submitted by

Nathan A. Green

This thesis has been read by each member of the following graduate committee and by majority vote has been found to be satisfactory

\_\_\_\_\_  
Date

\_\_\_\_\_  
Gordon W. Romney, Chair

\_\_\_\_\_  
Date

\_\_\_\_\_  
Barry M. Lunt

\_\_\_\_\_  
Date

\_\_\_\_\_  
Joseph J. Ekstrom



BRIGHAM YOUNG UNIVERSITY

FINAL READING APPROVAL

I have read the thesis of Nathan A. Green in its final form and have found that (1) its format, citations, and bibliographical style are consistent and acceptable and fulfill university and department style requirements; (2) its illustrative materials including figures, tables, and charts are in place; and (3) the final manuscript is satisfactory to the graduate committee and is ready for submission to the university library.

\_\_\_\_\_  
Date

\_\_\_\_\_  
Gordon W. Romney  
Chair, Graduate Committee

Approved for the Department

\_\_\_\_\_  
Thomas L. Erekson  
Director, School of Technology

Accepted for the College

\_\_\_\_\_  
Alan R. Parkinson  
Dean, Ira A. Fulton College of  
Engineering and Technology



## ABSTRACT

### ESTABLISHING PUBLIC CONFIDENCE IN THE VIABILITY OF FINGERPRINT BIOMETRIC TECHNOLOGY

Nathan A. Green

School of Technology

Master of Science

The most common personal authentication techniques used for identity management employ a secret PIN or password that must be remembered. The challenge, for a given user, is that a multitude of such codes must be recalled over the course of the day for transactions involving distinct computer applications. Password mania prevails. Fingerprint biometric technology is an ideal alternate solution to this password recall problem. In spite of their availability for nearly thirty years, fingerprint biometric systems still remain uncommon in public sectors of industry such as education, government, and technology. Technology has improved sufficiently that false acceptance and rejection rates are no longer valid excuses. Two proposed reasons for this lack of deployment are 1) society's misunderstanding regarding the personal privacy, security, and function of the technology; and 2) inadequate education regarding the technology. This present





research was structured to test these hypotheses, and attempt to identify the major societal factors that have limited fingerprint biometric deployment in IT authentication systems. Three research approaches regarding acceptance of fingerprint biometric technology by targeted populations were used in this study, namely 1) a personal survey, 2) a personal training exercise, and 3) a web-based survey. Targeted populations included the general public in the State of Utah and its legislative members who made decisions regarding identity management legislation for state departmental functions. Objectives of this research included gaining a better understanding of 1) legislator's perceptions of why past legislation was rejected, and 2) the public's perception of the personal security of the technology. An additional objective was the confirmation that proper education on security issues improves personal confidence in and acceptance of fingerprint biometric technology.



## ACKNOWLEDGMENTS

I would like to express my profound appreciation to my Graduate Committee for their concern, input and efforts. I'd like to especially give thanks to Dr. Gordon Romney for being an advocate and mentor throughout the whole thesis-writing process. I express my deepest love and appreciation to my wonderful wife Cami for her patience, encouragement, and companionship, and also to my beautiful daughter Ellie.



## TABLE OF CONTENTS

LIST OF FIGURES.....	xvii
LIST OF TABLES.....	xviii
<b>CHAPTER 1 – INTRODUCTION</b> .....	19
1.1 Topic Introduction .....	19
1.2 Statement of the Problem.....	19
1.2.1 Cost .....	20
1.2.2 Availability .....	20
1.2.3 Accuracy .....	21
1.2.4 Speed.....	21
1.2.5 Convenience.....	22
1.2.6 User Acceptance Issues.....	22
1.2.7 Overcoming Negative User Perceptions.....	23
1.3 Hypothesis.....	23
1.4 Assumptions.....	24
1.5 Thesis Structure .....	24
1.5.1 Literature Review.....	24
1.5.2 Research Methodology .....	25
1.5.3 Research Results and Analysis .....	25
1.5.4 Conclusions.....	26
1.6 Significance of the Study .....	26
1.7 Delimitations.....	28
1.8 Glossary of Terms.....	29
<b>CHAPTER 2 – REVIEW OF LITERATURE</b> .....	31
2.1 Social Issues.....	31
2.1.1 Security Concerns .....	32
2.1.2 Privacy Concerns .....	33
2.1.2.1 Third Party Data Accessibility.....	34
2.1.2.2 Loss of Identity .....	35
2.1.3 Cultural and Religious Stigmas .....	36
2.1.4 Health Concerns.....	38
2.1.5 Past Research Regarding User Acceptance .....	39
2.1.5.1 Public Acceptance of Biometric Usage .....	39
2.1.5.2 Biometrics Usage within Electronic Business .....	41
2.1.6 Overcoming User Perceptions .....	41
2.2 Legal Issues.....	43
2.2.1 The Fourth Amendment.....	44

2.2.2 The Privacy Act of 1974 .....	44
2.2.3 Other National Legislation.....	45
2.2.4 Fingerprinting Law Suits .....	46
2.2.5 Future Legal Considerations .....	48
2.3 Human Factors .....	49
2.3.1 Fingerprint Individuality .....	49
2.3.2 Gender Factors .....	50
2.3.3 Age Factors .....	50
2.3.4 Ethnicity Factors .....	50
2.3.5 Occupational Factors .....	51
2.3.6 Percentage of Population Unable to Enroll.....	51
2.3.7 Further Human Factors Considerations .....	52
2.4 Technical and Implementation Issues .....	52
2.4.1 Fingerprint Biometric Performance .....	53
2.4.2 History of Fingerprint Usage .....	54
2.4.3 Fingerprint Biometric Cost and Availability .....	55
2.4.4 Convenience of Fingerprint Biometrics.....	55
2.4.5 Implementation Issues .....	56
2.4.5.1 User Training and Education .....	57
2.4.5.2 Enrollment Process .....	58
2.4.5.3 Sensor Placement .....	59
2.5. Security Issues .....	59
2.5.1 Points of Vulnerability.....	60
2.5.2 Vulnerability Studies .....	61
2.5.3 Liveness Detection.....	62
2.6 Summary .....	62
<b>CHAPTER 3 – RESEARCH METHODOLOGY .....</b>	<b>63</b>
3.1 Introduction.....	63
3.1.1 Introduction of Phase One .....	63
3.1.2 Introduction of Phase Two.....	64
3.1.3 Introduction of Phase Three.....	64
3.1.4 Introduction of Phase Four.....	65
3.2 Phase One.....	66
3.2.1 Locating Necessary Hardware and Software.....	66
3.2.1.1 NIST Public Domain Fingerprint Software .....	67
3.2.1.2 MINDTCT .....	68
3.2.2 Converting Scanned Image to NIST’s AN2K Format.....	70
3.2.2.1 Type-14 Variable-Resolution Record Layout.....	71
3.3 Phase Two.....	73
3.3.1 Sample Population .....	74
3.3.1.1 Appropriateness of Population Selection.....	74
3.3.1.2 Random Sampling.....	75
3.3.1.3 Sample Size.....	76
3.3.1.4 Involvement of Survey Experts .....	77
3.3.2 Survey Questions .....	77
3.4 Phase Three.....	83
3.4.1 Technology Overview.....	84
3.4.2 Online Survey .....	85

3.5 Phase Four.....	87
3.5.1 Questions Asked of Representatives.....	88
3.5.2 State of Utah CIO.....	90
<b>CHAPTER 4 – RESEARCH RESULTS .....</b>	<b>91</b>
4.1 Phase One Results.....	91
4.1.1 Fingerprint Extraction Process.....	91
4.1.2 Conclusions of Phase One .....	95
4.2 Phase Two.....	95
4.2.1 Demographic Data .....	95
4.2.2 Question 1 .....	96
4.2.3 Questions 2-4.....	97
4.2.4 Question 5 .....	97
4.2.5 Question 6 .....	98
4.2.6 Question 7 .....	99
4.2.7 Question 8 .....	99
4.2.8 Question 9.....	100
4.2.9 Question 10 .....	101
4.2.10 Question 11 .....	101
4.2.11 Question 12.....	102
4.2.12 Question 13 .....	103
4.2.13 Question 14.....	104
4.2.14 Question 15 .....	105
4.2.15 Question 16.....	105
4.2.16 Question 17 .....	106
4.2.17 Question 18.....	107
4.2.18 Conclusions of Phase Two.....	108
4.3 Phase Three.....	111
4.3.1. Demographic Information.....	111
4.3.2 Questions from Original Survey .....	112
4.3.2.1 Question 1 .....	112
4.3.2.2 Question 2 .....	113
4.3.2.3 Question 3 .....	113
4.3.2.4 Question 4 .....	114
4.3.2.5 Question 5 .....	114
4.3.2.6 Question 6 .....	115
4.3.2.7 Question 8 .....	115
4.3.2.8 Question 9 .....	116
4.3.2.9 Question 10.....	116
4.3.2.10 Questions 11-12 .....	117
4.3.3 Additional Survey Questions .....	117
4.3.3.1 Question 7 .....	117
4.3.3.2 Questions 13-14 .....	118
4.3.3.3 Question 15 .....	119
4.3.4 Conclusions of Phase Three.....	119
4.4 Phase Four.....	123
4.4.1 Contacted Representatives.....	123
4.4.2 Issues and Voting on the Bill.....	124
4.4.3 Identity Theft and Privacy Invasion.....	125



4.4.4 Summary of State of Utah CIO Comments .....	126
4.4.5 Conclusions.....	127
<b>CHAPTER 5 – CONCLUSIONS</b> .....	129
5.1 Summary of Conclusions.....	129
5.2 Results of Hypothesis .....	131
5.3 Suggestions for Further Study .....	136
5.4 Summary .....	138
<b>BIBLIOGRAPHY</b> .....	141
<b>APPENDICES</b> .....	145
APPENDIX A.....	147
Survey 1 Questions .....	147
Survey 1 Data.....	148
Demographic Information.....	150
Graphs of Phase Two Survey Responses.....	151
Results Based on Technical Expertise .....	156
Results Based on Gender .....	158
Results Based on Age .....	161
Results Based on Education Level.....	163
Results Based on Occupation.....	165
Results Based on Demonstration .....	168
APPENDIX B .....	171
Survey 2 Questions Data.....	171
Survey 2 Data.....	172
Graphs of Phase Three Survey Results.....	174
Comparison of Phase Two and Phase Three Responses.....	177
APPENDIX C .....	181

## LIST OF FIGURES

<b>Figure 2.1:</b> Public perceptions of acceptable uses of biometrics .....	39
<b>Figure 2.2:</b> Number of respondents uncomfortable with various biometric technology .	40
<b>Figure 3.1:</b> Targus Defcon biometric authenticator .....	66
<b>Figure 3.2:</b> NIST's MINDTCT minutiae detection process .....	68
<b>Figure 3.3:</b> Fingerprint image before binarization (left) and after binarization (right) ...	69
<b>Figure 3.4:</b> Pixel patterns used to detect minutiae .....	70
<b>Figure 3.5:</b> ATImageCapture software screen capture .....	70
<b>Figure 3.6:</b> Minutiae and direction superimposed over a fingerprint image.....	73
<b>Figure 3.7:</b> Facts of fingerprint biometric technology .....	84
<b>Figure 4.1:</b> Transform.bat – script for transforming bitmap image to usable raw format.....	92
<b>Figure 4.2:</b> Extract.sh – script for calling txt2an2k and mindtct for viewing fingerprint image data.....	92
<b>Figure 4.3:</b> Nist3.fmt – formatted text file inputted into TXT2AN2K for minutiae extraction.....	93
<b>Figure 4.4:</b> Data from minutiae-extraction process .....	93
<b>Figure 4.5:</b> MINDTCT minutiae data format .....	94
<b>Figure 4.6:</b> Respondents answering favorably in both surveys .....	120

## LIST OF TABLES

<b>Table 2.1:</b> Drawbacks of various biometric technologies.....	53
<b>Table 2.2:</b> Error rates summarized from scenario and technology evaluations .....	54
<b>Table 3.1:</b> Type-14 variable-resolution tenprint record layout .....	72
<b>Table 4.1:</b> Difference in favorable responses from Phase II to Phase III.....	120
<b>Table 4.2:</b> Standard deviation and effect size analysis table.....	122

## CHAPTER 1 –INTRODUCTION

### 1.1 Topic Introduction

In an October 2004 article in SC Magazine, the topic of biometrics is discussed and the following statements are made: “How many individuals in your office are using biometrics on a daily basis? This situation begs the question as to why we are yet to see widespread use of biometrics in the typical office environment...Perhaps it has more to do with trust in what, to many, is still an emerging technology. Or, perhaps it is simply a lack of awareness of how this technology works and its benefits.”[27] This raises interesting questions about why biometric technology is not more prevalent; particularly fingerprint biometric technology which has been around in early forms since the early 1970s.

### 1.2 Statement of the Problem

Automated fingerprint recognition was first developed by the FBI in the late 1960s and implemented in the early 1970s. Since that time, the technology has matured and been perfected such that it has been reduced dramatically in price and increased in reliability. Why then has biometric fingerprint technology not become mainstream in society and commerce as an identity management tool, particularly within industries

where identity management and security is paramount? Like any identity management technology, fingerprint biometric technology can be described in terms of system cost, availability, accuracy, speed, convenience, and user acceptance.

### 1.2.1 Cost

Fingerprint scanning technology was not commercially available and was very expensive when first invented. It was used by the FBI as a way to search and validate fingerprints automatically. Because fingerprint scanning technology has been available for roughly 30 years, costs have fallen sharply. In fact, modern fingerprint scanners can be purchased for as little as \$25 on the Internet. Most scanners are bundled with software and drivers to handle the device and could be suited to handle more complex identity management needs. More durable and advance scanners would obviously cost more, however such cost would not surpass existing identity management systems such as smart card readers or other magnetic media. Therefore, it can be concluded that hardware price obviously is not a major issue.

### 1.2.2 Availability

In addition to being inexpensive, fingerprint biometric hardware is readily available. By going to Google.com and searching for 'fingerprint scanner', dozens of different vendor-sites are returned with a variety of different biometric fingerprint hardware solutions available. Most computer accessory retailers like CompUSA and Circuit City offer similar hardware as well. Clearly, the technology is readily available to the general public.

### 1.2.3 Accuracy

How accurate are current fingerprint scanners? Accuracy is usually defined in terms of false acceptance rates (FAR), which is the measure of the likelihood that the biometric security system will incorrectly accept an unauthorized person, and false rejection rates (FRR), which is the measure of the likelihood that the system will incorrectly reject an access attempt by an authorized user. A recent fingerprint verification benchmark competition had best and worst case FRR and FAR of fingerprint verification technology at .0001-.01% and .3-.7% respectively. [24] Compared to other biometric technologies like face, voice, iris, hand, and signature, fingerprint biometrics has the lowest FAR and one of the lowest FRR of the technologies. [4] These numbers show that fingerprint biometric technology is quite accurate when compared to other biometric technologies and probably accurate enough to replace existing security measures for access to computers or buildings.

### 1.2.4 Speed

Accuracy is important in any identity management solution, but system speed is equally important. In the same fingerprint verification competition mentioned above, some algorithms were able to both enroll fingerprints and identify them in times just slightly over 1 millisecond. [24] Commercially available systems usually have verification speeds averaging about one second, which is sufficiently fast for most applications.

### 1.2.5 Convenience

Fingerprint biometric convenience is one of the greatest advantages of the technology. Because a biometric is a measurable feature, it does not need to be remembered, hidden, replaced, or repaired. Fingerprint biometrics has all of these qualities and is unquestionably more convenient than the majority of all other non-biometric identity management technologies. Time and costs associated with password-resets and security-access media purchase and encoding could be greatly reduced or eliminated by converting to a fingerprint-based biometric system

### 1.2.6 User Acceptance Issues

If all of the above factors are not the cause of the lack of proliferation, then user acceptance must be the root cause. Experts in the field of biometric technology have said: “Fingerprint technology is in the middle of the scale (or low) as far as its acceptance to the general public is concerned. Much of this lukewarm acceptance is due more to perception than reality.”[1] Julian Ashbourn, a leading expert in the field of biometrics said, “Primary among [technical factors] are perhaps human factors...We are, after all, considering applications in which humans play a very significant part, otherwise, why would we be considering automated biometric identity checks? User psychology factors are relevant not just in everyday operation, but throughout the whole project, including the initial communication to prospective users and their subsequent registration into the system.”[2]

If user perceptions and social issues are one of the root causes for the technology not to be more widespread, then what are the specific issues and user perceptions preventing the technology from being implemented and how can they be overcome? This

is precisely the question this thesis attempts to answer. This thesis focuses on determining the negative social perceptions hindering the proliferation of fingerprint biometrics.

### 1.2.7 Overcoming Negative User Perceptions

Once these perceptions are identified and enumerated, what can be done to overcome them? Many of the problems with regard to fingerprint biometrics exist within the realm of users' false perceptions and misconceptions of the technology. Because such perceptions are not always based in reality or upon factual data, education possibly can be used to advance acceptance of the technology. [1] According to some researchers, the best way to overcome a user's preconceived negative impressions of a system is good communication. The user's concerns need to be addressed and the system's use and benefits needs to be enumerated. [2] Therefore, this thesis seeks to determine the level to which educating users can favorably alter negative perceptions of fingerprint biometric technology.

### 1.3 Hypothesis

This research postulates that a population that has received education regarding scientifically established facts of fingerprint biometric technology would exhibit higher levels of acceptance and understanding of the technology and lower levels of concern when compared to the uneducated. The level of acceptance would be measured as a percentage of the surveyed population compared to the level measured previous to education. This hypothesis is based on two assumptions that require evaluation.



## 1.4 Assumptions

The first assumption was that social impediments are the major factor in the low adoption of fingerprint biometrics as opposed to those other factors mentioned above such as system cost, accuracy, speed, and convenience. These factors are not identified as major limitations to the advance of fingerprint biometric technology. Data and research supporting this assumption is presented in Chapter 2 along with a review of the outstanding issues of the technology and an indication of where further research might be conducted.

The second assumption was that a portion of the general population holds misconceptions regarding fingerprints and fingerprint biometrics. This assumption was central since much of the research carried out involved determining the perception of fingerprints and fingerprint biometrics held by certain portions of the general population through a series of interviews.

## 1.5 Thesis Structure

### 1.5.1 Literature Review – Chapter 2

This thesis begins with a review of literature covering the major issues relating to potential barriers to fingerprint biometric technology proliferation. The review mainly focuses on the perceived social issues with the technology, commentary and research previously conducted in the area and the need for further research in this area. Legal concerns and past litigation on privacy issues regarding fingerprints and biometric technology are also explored. Human factors and their potential effect on biometric

technology proliferation and the extent to which they play a part in fingerprint biometric proliferation are noted in the literature review. Technical and implementation issues, including comparisons of fingerprint biometric technology with other biometric solutions, are also mentioned in the literature review. Issues of security relating to fingerprint biometrics and research done in that area are examined as well.

### 1.5.2 Research Methodology – Chapter 3

Following the review of literature, the thesis specifies the research method by which the social issues were researched and outlines the means whereby these issues could be overcome. This chapter covers the four main areas of the research, namely (1) exploring hardware and software to view the inner-workings of the fingerprint feature extraction process and reproducing that process for the benefit of education, (2) administering an interview-style survey among technology, education, and government populations in the state to determine the level to which certain social biases concerning fingerprint and biometric usage exist, (3) administering a combined web-based education and survey program to determine the level to which educating users on the facts of biometric fingerprint technology lowers the level of concern about the technology, and (4) gaining an authoritative opinion from Utah State legislators on previous attempts to implement identity management technology on a state-wide level.

### 1.5.3 Research Results and Analysis – Chapter 4

The next chapter of the thesis contains an enumeration of the research conducted and an analysis of the results relative to the main thesis research question – ‘If user perceptions and social issues are the root causes for the technology not to be more

widespread, then what are the specific issues and user perceptions preventing the technology from being implemented and how can they be overcome?’ Conclusions as to the significance of the results are also be specified in this chapter.

#### 1.5.4 Conclusions – Chapter 5

Following the chapter on the results of the research, final conclusions are discussed and the research is summarized. This section also reviews further areas of study in the field of fingerprint biometric proliferation and user acceptance which could be undertaken.

#### 1.6 Significance of the Study

The goal of this research was to help facilitate fingerprint biometric technology to cross the chasm from currently being a misunderstood novelty to a widespread, mainstream personal identity authentication tool. The geographical demographic focused upon in the research was limited to the general Salt Lake and Utah County areas within the state of Utah. New identity management technologies with the potential to secure personal information would likely be embraced by most individuals, particularly in this time of great identity theft concern. In a survey done by Entrust, Inc of 2,000 Internet users, 72% of users stated they would be willing to use an additional means of authentication to access their online bank accounts in order to improve the security of their identity.[30] This statistic indicates there is a desire for improved identity management technologies and security among the population. Fingerprint biometric technology is an under-utilized identity management technology. Julian Ashbourn, a

noted expert in biometric technology said, "...marketable electronic biometric devices have now been around for 15 years or so. Within this time, costs have fallen, matching algorithms have improved, and many suppliers have come and gone – and we are still sitting around talking about emerging technologies. This is a long gestation period.”[27]

This lack of utilization of biometrics can be seen in certain industries which would potentially benefit from it, specifically, technology, education, and government. For example, both Novell and the Utah State Parks and Recreation office use personal magnetic media to gain access to buildings and other secure resources. The inherent problems of lost and misappropriated media limit the reliability of this identity management solution. For fingerprint biometrics to become a more widely used identity management solution, negative user perceptions need to be understood and overcome. The research performed in this study could be applied as part of a large-scale enrollment procedure within education, technology, government, and possibly other organizations to help users become more comfortable and accepting of the technology.

The participants of the surveys were selected among the general population throughout different areas of Utah and will reflect demographics of varying age, technical expertise, and education. After information was gathered regarding user perceptions of the technology, it was compiled and analyzed to identify the major negative social perceptions regarding fingerprint biometric technology held by the surveyed population. After gathering this data, a concise and direct educational overview was compiled which included accurate facts for the purpose of refuting any possible misconceptions held about the technology. This information was shared with individuals in an online format. Following the distribution of the online-education, the level to which previous concerns changed was measured through the use of a brief online survey. The survey helped

quantify the effectiveness of the education and indicates whether or not it was an effective means of alleviating people's concerns. The results of this study could be applied to an organization attempting to implement a fingerprint biometric system. An organization could use the results of this study and apply them to the enrollment procedure for its biometric system in order to gain greater user acceptance, thus facilitating the technological implementation.

### 1.7 Delimitations

For the purpose of this study, the following conditions were identified as variables that were not statistically evaluated as significant factors nor considered in the final analysis:

1. The surveyed population study was limited to individuals residing in the State of Utah, specifically Salt Lake or Utah County,
2. Because of their size, presence, and number of employees, Novell, Brigham Young University (BYU), and the Utah State Parks and Recreation were considered representative of technology, education, and government offices.
3. Demographic information was used in the analysis of Phase II to assure the targeted population is diverse and is representative of a variety of backgrounds. Though the demographic information is also used somewhat in the analysis of the Phase II results, it was not gathered for this purpose and was not considered in Phase III of the research.

## 1.8 Glossary of Terms

**Bifurcation:** The splitting or branching of two fingerprint ridges.

**Biometrics:** A method of verifying an individual's identity based on measurement of the individual's physical feature(s) or repeatable actions where those features and/or actions are both unique to that individual and measurable.

**FAR:** The measure of the likelihood that the biometric security system will incorrectly accept an access attempt by an unauthorized user.

**FRR:** The measure of the likelihood that the biometric security system will incorrectly reject an access attempt by an authorized user.

**IC Chip:** A small electronic device made out of semiconductor material for storing electronic information.

**Ridge Ending:** The point at which a fingerprint ridge ends.

**Spoofing:** Pretending to be someone else. The deliberate inducement of a user or a resource to take an incorrect action.



## CHAPTER 2 – REVIEW OF LITERATURE

The literature review addresses five areas of the research problem: (1) social issues and user perceptions pertaining to the use of fingerprint biometrics, (2) legal implications related to fingerprint biometrics, (3) human factors relating to the technology, (4) technical and implementation issues related to fingerprint biometric systems, and (5) security issues. This review highlights the various issues of the technology, research previously conducted in the area, commentary and other notable literature. It highlights where the greatest unresolved issues lay and indicates where further research might be conducted.

### 2.1 Social Issues

Social issues such as misconceptions, misunderstandings, and hesitations tied to fingerprint biometric technology implementation and utilization may comprise the most significant barriers to the technology's proliferation. Fingerprint biometrics tend to be inferior to all other common biometrics in terms of its intrinsic properties. [4] As with any technology, if a user population has personal security uncertainties or believes the technology is intrusive in any way, the technology will likely be unaccepted and go unused. Similarly, individuals' conceptions of what fingerprints in a fingerprint biometric system will be used for will greatly impact whether the system is accepted, and



will ultimately determine the degree to which the technology will be embraced by the general public. In terms of social acceptance, fingerprint biometric technology ranks low to medium when compared to other biometric technologies. Acceptance is largely based on the ease of enrollment and is an apparent threat to personal privacy. [1] Previous research has not determined the degree to which social acceptance or lack of acceptance of fingerprint biometric technology exists. Therefore, further research should be undertaken to understand what reservations exist among the general population.

If a user were to believe that a biometric identifier could be shared or accessed by a third party or used for undisclosed purposes, user acceptance of the system will likely be low. Many of the problems regarding fingerprint biometrics exist within the realm of users' false perceptions and misconceptions of the technology. Because such perceptions are not always based in reality or upon factual data, education can be used to advance acceptance of the technology. [1] The key to increasing the technology's acceptance is to figure out how such perceptions can be alleviated. According to some researchers, the best way to overcome a user's preconceived notions of a system is good communication. The user's concerns need to be addressed and the system's use and benefits needs to be enumerated. [2] Before any type of education can be designed to effectively help users accept the technology, all potential concerns of the users must be understood.

### 2.1.1 Security Concerns

No security or identity management system can be entirely foolproof, including fingerprint biometric systems. Security and concerns over protecting personal identity are major issues to consider when implementing a fingerprint biometric system.

Fingerprints are more difficult to steal and copy than a password, but the level of

intrusiveness is largely based upon the user's perception of the system's security. A finger on a sensor would likely be seen as superior to typing in a password in terms of time and memorization required. However, obtaining a fingerprint by using an electronic sensor could be perceived as an invasion of privacy. Therefore, user acceptance and level of intrusiveness are very closely related. It is important to emphasize to users that "fingerprint templates are algorithmic representations of a fingerprint but cannot be used in reverse fashion to re-create the pattern of a fingerprint." [1] Understanding this may help to reduce the level of perceived security risk and bolster the level of perceived security of fingerprint biometric systems.

The accuracy and dependability of fingerprint biometric systems are often measured in terms of False Acceptance Rates, False Rejection Rates, and other rates of error. Because of this method of measurement, there is a common misconception that biometric technology is weaker in terms of security when compared to a password-based system. Because passwords can be broken by brute force, social engineering, or sharing with the wrong person, fingerprint biometric technology should be considered more secure and reliable for accurately identifying individuals than password-based authentication systems. [1]

### 2.1.2 Privacy Concerns

Privacy concerns are a source of potential concern. Though we leave fingerprints all over the place on a day to day basis, when an individual is enrolled in a fingerprint biometric system he may worry about an invasion of privacy. A potentially major social concern is the fear of a "big-brother" type scenario in a fingerprint biometric system. A notable expert in the field of biometrics said, "Any high-integrity identifier represents a

threat to civil liberties, because it represents the basis for a ubiquitous identification scheme, and such a scheme provides enormous power over the populace. All human behavior would become transparent to the State, and the scope for nonconformism and dissent would be muted to the point envisaged by the antiutopian novelists.”[15] The fear exists among some that slowly over time, biometric identification systems would evolve and overlap to the point where unintended and potentially harmful uses could come about. [3] Researchers have expressed that such a concern exists in society, but a quantitative measure needs to be determined.

#### 2.1.2.1 Third Party Data Accessibility

Other concerns regarding privacy and fingerprint biometrics exist according to some publications. When fingerprint biometric data is read from an individual, information about that person is stored in a database and is used to identify her at a later time. This information is stored in a digital form which can be deleted, copied, or duplicated almost instantly assuming access to the data is available. This is the basis for another potential privacy concern regarding fingerprint biometrics. Individuals appear to fear that their digitally-stored biometric information could potentially be copied many times over, shared with third parties, or even sold to people willing to pay to use it illegally. The same biometric information used among the private sector could potentially be accessed by federal or state law enforcement agencies looking for criminals. Privacy could be perceivably invaded when surrendering a personal identifier like a fingerprint to an organization. The concern that data can be shared with other organizations’ databases such as government or law enforcement agencies persists. Fingerprints can be matched against various databases currently through the FBI and INS

systems. The fear that publicly or privacy administered biometric systems could interface with these systems increases the perceived threat of personal privacy invasion. [7] Additionally, the idea that private information could be obtained about an individual based solely on the digitally stored biometric signature is alarming to some. [3] However, some states, including California, Maryland, and Virginia, were successful in prohibiting the collection and distribution of biometric data without the knowledge and consent of the subject. [4] The degree to which third party data accessibility exists among the population needs to be determined through further research. All of the aforementioned privacy issues are likely to be significant to some individuals. All of these privacy concerns combined could lead many to believe that a fingerprint biometric system is not a viable technology and intrudes on one's right to personal privacy. Privacy issues related to fingerprint biometrics would need to be carefully addressed for users for any entity employing such a system.

#### 2.1.2.2 Loss of Identity

Identity theft is another potential area of concern. It should be understood that while fingerprint biometrics are used to link an identity, they are not used as an alternate or replacement identity. A fingerprint sensor used to secure an area would authenticate individuals enrolled in the system upon request. However, an identity cannot be stolen merely by having a copy of an authorized user's fingerprint, though unauthorized access to the secure area could be granted. Though fingerprint biometrics should not be associated with identity theft, critics of biometrics wage a variety of privacy-related arguments against the technology in addition to those issues raised above. A common criticism is that the use of biometric identifiers causes individuals to be stripped of their

anonymity whenever we enroll in a biometric identification system. In the minds of many, the use of a biometric feature is dehumanizing, giving individuals the perception of becoming nothing more than a fingerprint. Such individuals feel that being identified within a matter of seconds by their fingerprint is belittling and dominating. Such feelings would constrain or prevent a fingerprint system from being accepted among a population. [15] Another related fear stemming from fingerprinting and biometric identification is the perceived similarity it has with branding or tattooing. A tattoo or brand is used to identify an individual among a population. Similarly, a fingerprint can be used in a biometric identification system to accurately identify an individual. Since branding of individuals is widely considered controversial and has taken place in human history, as in times of slavery, the fear that people could be treated in a similar fashion through the abuse of identifying features in a biometric system could exist. [3]

### 2.1.3 Cultural and Religious Stigmas

Aside from the privacy-related social issues are the cultural concerns and stigmas which exist regarding the use of fingerprints for identification purposes. In many cultures, the use of fingerprints has a poor reputation and is associated with criminal activity or other types of wrongdoing. This poor reputation may be attributed to the strong relationship between criminal history and fingerprinting. In some cultures where fingerprints are used in place of signatures such as the Mayan culture, fingerprints are associated with illiteracy. [4]

Certain ultra-conservative and religious groups see biometrics and other identity management tools as inherently evil. Many of these groups base their perception of these identity management tools on an interpretation of a portion of the Book of Revelation in

the New Testament: “And he causeth all, both small and great, rich and poor, free and bond, to receive a mark in their right hand, or in their foreheads: And that no man might buy or sell, save he that had the mark, or the name of the beast, or the number of his name. Here is wisdom. Let him that hath understanding count the number of the beast: for it is the number of a man; and his number is Six hundred threescore and six.”[5]

These religious groups see biometrics as the ‘mark of the beast’ mentioned in the Book of Revelation. One such noteworthy group is the Eagle Forum—an extreme right-wing organization known for speaking out on privacy and identity management-related issues and lobbying lawmakers to influence votes. On an identity management issue similar to biometric technology, the National ID card, Phyllis Schlafly of the Eagle Forum said: “...This type of personal surveillance is the indicia of a police state. It operates as an efficient watchdog to stifle any emergence of freedom.”[6] Identity management technologies are sensitive issues with many opponents and ultra-conservative groups willing to fight against related legislation because of the perception of major privacy invasions. Biometric fingerprint systems would likely come under similar criticism by such groups if proposed on a large-scale.

A large-scale deployment of an identity management system related to fingerprint biometric technology was debated in the State of Utah in early 1997. Smart card technology was suggested for application in Utah State Driver’s Licenses. The smart card driver’s licenses would have contained an IC chip which could store detailed identifying information about the card’s holder. Though the technology has been accepted and utilized by many around the world, it was rejected by segments of the Utah population. In February 1997, Utah legislators attempted to pass identity management legislation mandating the use of smart-card technology in driver’s licenses. Though

passing the initial vote in the House of Representatives by a margin of 43 to 23, it made it to the interim study calendar of the Utah Senate and was never further discussed or pursued. As is seen in Chapter 4 of this thesis, the defeat of the legislation was mostly due to opposition by both extreme left and right-wing organizations who claimed privacy would be invaded by implementing the technology. Though not dealing with fingerprint biometrics directly, this issue relates to capturing and storing personal information and illustrates that identity-management technologies are often misunderstood and requires additional education to proliferate.

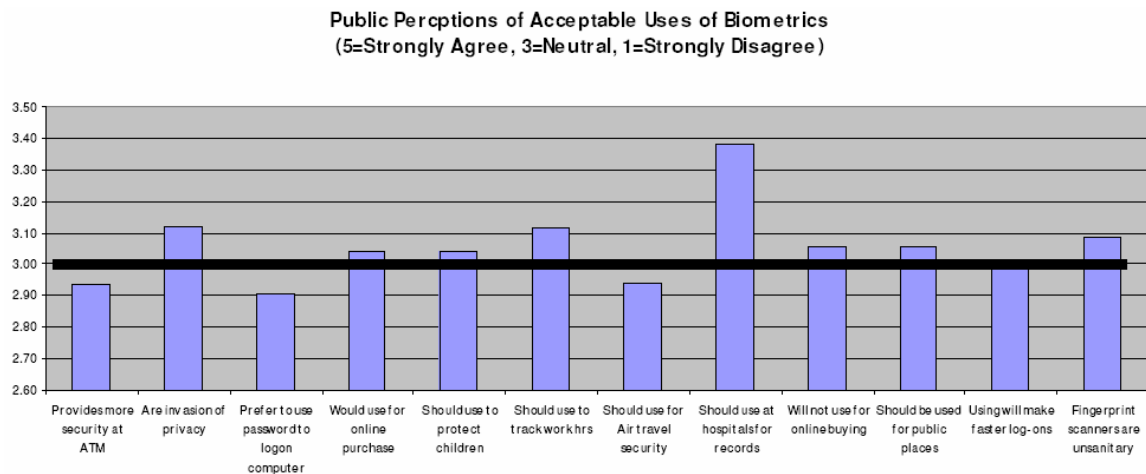
#### 2.1.4 Health Concerns

As strange as it may sound, the issue of the health-related safety of fingerprint scanners is another potential concern with the technology. Because direct, physical contact is required between a user's finger and the device's sensor, the fear of spreading germs, getting an electrical shock, or experiencing other pain may exist. The required contact between a large number of users and a single sensor device would be seen by some as a perceived health risk and would reduce user acceptance. One of the best ways to circumvent this problem is to remind people of the daily interaction taking place between people and everyday objects. For example, hundreds of people may use the same door handle or press the same elevator button on a daily basis and have no concerns with it. The concern of germs or other hazards related to the use of fingerprint scanners should be perceived in a similar, non-intrusive manner. [1]

## 2.1.5 Past Research Regarding User Acceptance

### 2.1.5.1 Public Acceptance of Biometric Usage

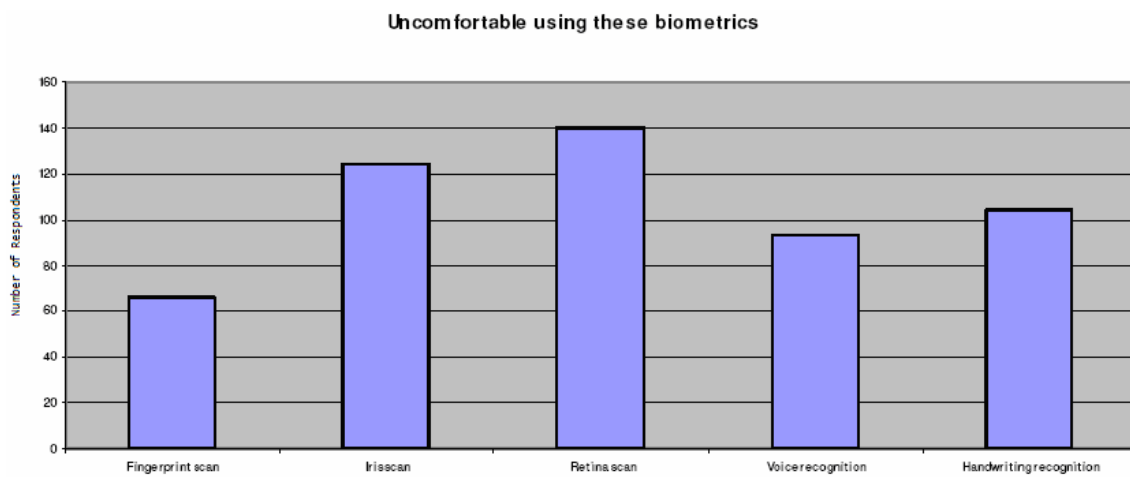
The degree to which the general population has concerns with biometric technology is important to study. Little research with specific focus on fingerprint biometric technology has been performed. One study focusing on various types of biometrics was undertaken by Janette Moody of the international journal Informing Science. The research focused on the use of biometrics currently implemented in organizations, public perceptions of various biometric technologies, and suggestions for educating the population. A survey was conducted on a population of approximately 300 individuals and sought to determine the general population's opinions of the types of preferred biometrics and the preferred usages of these biometrics. Figure 2.1 below is a graph taken from the study showing the public's perceptions of the acceptable use of biometrics. [23]



**Figure 2.1:** Public perceptions of acceptable uses of biometrics [23]



According to the study, biometrics used for hospital records are the most acceptable use for biometrics. However, biometrics are still perceived as an invasion of privacy. When asked about the types of biometric technology which seemed most intrusive and would make the population the most uncomfortable, the population responded by finding fingerprint scanning as the most acceptable of the technologies asked about. This data is shown in Figure 2.2.



**Figure 2.2:** Number of respondents uncomfortable with various biometric technology [23]

This study indicates that there are still concerns over the acceptable uses of biometric technology and how they should be used, but suggests that fingerprint scanning is the biometric technology the population is most comfortable with. It is important to recall that in the over thirty years the technology has existed, it has not become widely accepted in society or commerce. Therefore, research focusing specifically on fingerprint biometrics and the population's concerns with the technology needs to be conducted.

#### 2.1.5.2 Biometrics Usage within Electronic Business

Another study relating to the topic of user perceptions of biometric technology was a master's thesis titled "User perceptions related to identification through biometrics within electronic business." by Giesing. As part of the research performed, focus groups were held to gain an understanding of some of the perceived problems with the technology in an electronic business setting. Highlighted among his findings were the importance of carefully selecting the proper type of biometric technology, trusting the biometric identification method selected, and considering the selected biometric technology's intrusiveness. Giesing also concludes that "user perceptions with regard to security and privacy considerations were identified as social factors that need to be addressed as part of user adoption when making use of biometrics as an identification method within Electronic Business." [25] He also concludes that there appears to be a general uncertainty regarding biometric technology implementation, and further research could be conducted in many areas.

#### 2.1.6 Overcoming User Perceptions

Clearly there is a number of potential, widely-held concerns regarding fingerprint biometric technology. In order for fingerprint biometric technology to become more widely adopted, user's concerns need to be overcome. Experts have pointed out the importance of determining how large-scale biometric authentication system deployment can work on a large-scale "without creating additional security loopholes, and without infringing on civil liberties." [4] It has been noted that to overcome negative notions of fingerprint biometric technology, the enrollment and verification process should be

covered with users, along with why the process is setup the way it is and what the user needs to do to be enrolled in an acceptable way. [2]

The social biases and negative user perceptions mentioned in this review are not always based upon facts nor in reality. Therefore, education can be used to help advance the popularity and overall acceptance of the technology. [1] Fingerprint biometric technology is a quick and efficient method of identifying individuals, but potential negative perceptions need to be overcome. While it is true that the possibility exists for biometrics to be exploited by groups with sufficient authority over and access to biometric data, the fact that biometrics could help to increase our level of privacy should be stressed. By replacing sensitive personal identifying information like social security numbers, date of birth, or passwords with biometric information, this sensitive information can be protected while simultaneously identifying the user. [4] It should also be clarified that fingerprints are nearly impossible to be stolen and replicated except by those with expert knowledge of the technology used in a particular system, whereas passwords, social security numbers, and keys can easily be stolen and used by the majority of the general public. Another example of alleviating fears through education is the fear that a biometric fingerprint system extracts and stores an entire fingerprint image. The image itself is not stored; rather, minutiae and other fingerprint features are extracted, transformed into a hash entry, compared, and stored in a database to identify users. While the method for this procedure varies by fingerprint biometric system, the overall process is the same. “Fingerprint templates are algorithmic representations of a fingerprint but cannot be used in reverse fashion to re-create the pattern of a fingerprint.”[1]

The American Association of Motor Vehicle Administrators made some insightful comments about smart-card identity management technology which should be applied to fingerprint biometric technology deployment. In a report on the smart card in driver's licenses legislation, they commented specifically about the opposition to smart card usage in the State of Utah: "There is certainly a lesson to be learned about public relations and customer education in the scenario. Technology is often misunderstood. People fear what they do not understand and are unfamiliar with. In order to overcome the fear of Big Brother or Satan being able to read your life history on a chip or manipulate your life, we need to learn a lesson and actively promote public education to gain understanding and acceptance of how the Smart Card will be used." [20] They suggest that there are ways to overcome false perceptions of technologies. Some of the issues which they believe should be discussed with users include (1) making the public aware of the chip cards in other applications, (2) explaining the ease of use, (3) explaining what information will be included and how and by whom it could be accessed, (4) training the public in the machine use of the card, (5) allaying the fear of privacy concerns (mistrust of government, in particular), and (6) explaining the convenience and accuracy of the card, its flexibility and ability to do more with one card. [20] These same issues can and should be discussed with would-be users of fingerprint biometric systems and would help instill the desired confidence in users to actively use the technology.

## 2.2 Legal Issues

As biometrics become more widespread, there is a growing concern over loss of privacy and the issue of data confidentiality. The concern is that as biometrics continue

to become more complex and widespread, personal information can be too easily tracked. Thomas Jefferson said “If we cannot secure all our rights, let us secure what we can.” [4] The legal issues involved with fingerprint biometrics are a source of concern that needs to be addressed.

### 2.2.1 The Fourth Amendment

People possess rights as to the use of their personal information. Fingerprints can uniquely identify individuals and should therefore be protected under similar laws. Thus, enrollees of fingerprint biometric systems should logically have certain rights pertaining to the use of their biometric data. Citizens of the United States have their privacy rights protected under the Fourth Amendment of the U.S. Constitution. Logically, there should be some protection of individuals fingerprint usage under the same amendment. The Fourth Amendment states: “The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.”[12] This amendment could be interpreted by some to include usage of biometric data as an object which could be seized illegally or against a person’s will.

### 2.2.2 The Privacy Act of 1974

Currently, there is not a specific law mandating the use of biometric technology. However, certain pieces of legislation exist which could have implications on the legal usage of fingerprint biometrics in both the public and private sectors. The Privacy Act of 1974 [13] was passed with the intention of regulating federal organizations and how they

obtain and use private information about their employees. This act was passed years before biometric technology was available. Nevertheless, the Privacy Act of 1974 may be applicable to individuals enrolling in a biometric system. The definitions section of the Privacy Act states “the term "record" means any item, collection, or grouping of information about an individual that is maintained by an agency, including, but not limited to, his education, financial transactions, medical history, and criminal or employment history and that contains his name, or the identifying number, symbol, or other identifying particular assigned to the individual, such as a finger or voice print or a photograph.”[14] A fingerprint easily fits the definition of a record as described in the act. The Privacy Act outlines certain measures which must be taken by data collecting agencies. These include protecting the collected data using technical, physical, or administrative measures in order to maintain the confidentiality of the records. A publication of the existence and character of the system of records is required by organizations which maintain individuals’ private data. Any time data is collected from an individual, it is the responsibility of the organization to inform him on (1) the authority who authorizes the disclosure of information, (2) the specific use of the collected information, (3) routine uses of the information, and (4) any effects which may exist by not providing any or all of the required information. [3]

### 2.2.3 Other National Legislation

There has been recent legislation which could ease any legal tensions regarding public biometric usage. With the heightened security resulting from the tragic terrorist attacks on the World Trade Center in 2001, new pieces of legislation have been put into effect which incorporates biometric identifiers in existing identification methods in order

to identify individuals. The Enhanced Border Security and Visa Reform Act were passed recently, mandating the requirement of a fingerprint in addition to entry papers to identify all foreigners entering the country. This act is meant to more greatly control border security and security in airports by identifying potential threats before they can enter the country. [3] A similar act, the Aviation and Transportation Security Act, proposes the use of biometric technology for increased security. For example, the act specifically mentions as part of new airport security measures, "...the use of biometric or other technology that positively verifies the identity of each employee and law enforcement officer who enters a secure area of an airport." [14] Other similar acts, such as the Government Paperwork Elimination Act and the Health Insurance and Accountability Act have been passed which allow biometric information to be used for validating personal information. [4] The federal government recently began an anti-terrorism program requiring truckers who haul hazardous materials to submit to fingerprinting. [8] While it has come under some criticism by civil liberty and other opposition groups, most feel it is a good security measure. Programs similar to these could help fingerprint biometric technology become more common and increase the population's familiarity with it.

#### 2.2.4 Fingerprinting Law Suits

A number of court cases and legislation dealing with fingerprint usage are noteworthy for this research. This legislation, while not addressing fingerprint biometric technology directly, closely relates to concerns and perceptions tied to the technology. The U.S. Supreme Court has mandated, "there is a realm of personal liberty which the government may not enter." [16] Privacy is recognized by the U.S. courts as physical

privacy, information privacy, and decision privacy. Most people would argue that we tend to be concerned about others' control of who can sense us, how information about ourselves is used, and the details of our personal identity. It is human nature for people to have an interest in knowing why, when, and to whom biometric information is disclosed. [3 p200] In recent years, there has been a number of significant court cases which deal with the issue of personal privacy in relation to fingerprints and fingerprint usage. The majority of the Supreme Court decisions in relation to this topic have mandated that individuals have limited privileges when it comes to their own fingerprints. In *Utility Workers Union of America v. Nuclear Regulatory Commission*, a group of utility workers challenged the Nuclear Regulatory Commission's (NRC) fingerprinting requirement for all workers claiming their collective Fourth Amendment rights had been violated. After hearing debate and argument from both sides, the court ruled that the fingerprinting procedure carried out by the NRC was minimally intrusive and did not merit an invasion of personal privacy. The case was eventually overturned and the NRC fingerprinting requirement remained. [17] This is an important case because it establishes that fingerprint acquisition could be considered legal when performed by an organization in a minimally intrusive manner, and therefore cannot be argued as an invasion of privacy. A similar case, *Christopher Ann Perkey v. Department of Motor Vehicles*, involved a claim that a fingerprint requirement on a driver's license had no relationship with the State of California's goal of keeping the highway's safe. The court ruled in favor of the Department of Motor Vehicles stating there was a rational relationship between the driver's safety and the use of the fingerprint on the driver's license. [9]



Another noteworthy case involved a family that was the recipient of assistance from the Temporary Family Assistance program. As part of the assistance program, recipients were required to provide their two index fingers for a biometric scan. This particular family refused to surrender their fingers to be scanned on the basis of religious beliefs, citing Chapter 13 of the Book of Revelation in the New Testament which talks about the ‘mark of the beast [5]’ required by the world in the future. Though the family believed having their fingerprints acquired and stored electronically was fundamentally wrong, the court ruled in favor of the defendant. After an appeal to the ruling, the family was granted an exemption from the fingerprinting requirement. [3] This case directly relates to fingerprint biometric technology. Though a special exception was made for the family after complaining about it, the court ruled that it was legal for the TFA to acquire a fingerprint and have it on file of the general population.

### 2.2.5 Future Legal Considerations

Privacy and legal issues will likely become more pronounced as biometrics become more widespread throughout society and commerce. These cases suggest that in the face of a legal battle over fingerprint usage in a biometric system, courts would likely rule in favor of the entity requiring the fingerprint sample as long as it is gathered non-intrusively and used for a legitimate purpose. However, some experts believe possible legislation hindering biometric usage could include preventing biometric data from being stored in public databases or giving individuals the right to not take part in a biometric identification scheme. [4] Such legislation would hinder the proliferation of the technology. It is likely that the legal debates connected with biometrics will never cease as long as biometrics are not widely accepted in society and commerce.

## 2.3 Human Factors

Human factors refer to the age, gender, ethnicity, and vocation of the biometric system's user population. Human factors have never been greatly recognized as areas of concern regarding fingerprint biometric technology. However, human factors play a role in the accuracy of fingerprint biometric technology and may play a small part in the level to which the technology is used in society and commerce.

### 2.3.1 Fingerprint Individuality

The two principles upon which fingerprint biometrics are deemed viable are: (1) fingerprints are permanent and (2) all fingerprints are unique and no two are exactly identical. The first principle stating the permanency of fingerprints has been validated by observation and is well established. However, in recent years the uniqueness of fingerprints has been challenged in court. While it has been shown that fingerprints are very likely unique for each person through observation, and even identical twins have fingerprints which are not identical [18], the scientific basis for the individuality of fingerprints has not been firmly established. [4] Studies have been performed which seek to establish the idea that all fingerprints are unique. One such study is based on modeling fingerprints in terms of fingerprint minutiae. The study concludes that the probability of falsely matching two different fingerprints is lower if the number of features per minutia is high, the resolution of minutiae for measuring a fingerprint is high, the number of query and reference fingerprints is low, and noise in the minutiae detection is low. [10]

### 2.3.2 Gender Factors

Regarding gender, women tend to have smaller fingers and longer fingernails than males. Because of the fingertip size difference, certain fingerprint scanner devices may have difficulty obtaining a good sample of a large fingerprint. However, this has not been proven conclusively and further research could be done to establish whether or not gender has a profound impact on the accuracy of fingerprint biometric systems. [2] Most current fingerprint scanners are able to accommodate fingers of every shape and size without regard to gender.

### 2.3.3 Age Factors

There are varying opinions as to the effect of an individual's age on the viability of fingerprint biometrics. As people age, their fingerprints becomes less and less pronounced due to the increased brittleness and decreased elasticity of the skin. Such degradation of the skin can result in poor fingerprint acquisition, template creation, and template matching from the original sample, necessitating re-enrollment of the user's fingerprint information. [2] The extent to which aging affects fingerprint acquisition and matching varies as a function of the type of sensor and hardware used.

### 2.3.4 Ethnicity Factors

The idea of ethnicity as a factor relating to the viability of fingerprint biometrics may well be the most controversial human factor issue. While some research has been conducted in the area, further research among various ethnic groups and over a large geographic area would contribute to an understanding of the effect of human factors on fingerprint biometric viability. It is believed that the extent of certain fingerprint patterns

varies throughout ethnic groups, but the connection between this belief and the performance of fingerprint biometric systems has not been well established. [2] The level to which ethnicity plays a role in the validity of fingerprint biometric technology may not be as strong as some believe. The technology is used all over the world in places like Europe and Asia, areas consisting of diverse ethnic groups, yet no major issues have been established for fingerprint biometric operation in these areas.

### 2.3.5 Occupational Factors

An individual's vocation is another factor contributing to the accuracy of fingerprint biometric systems. Certain vocations where manual labor or contact with abrasive chemical substances is required may result in the wearing of fingerprints. For systems which scan the most superficial surfaces of a finger, such vocations may hinder fingerprint biometric information capture. Many fingerprint scanning implementations overcome this barrier by scanning beneath the visible layer of the fingerprint and looking at the deeper layers of the skin. [2] Thus, depending on the type of hardware used and the work environment used in, scanner accuracy may be lower than it would be under different circumstances.

### 2.3.6 Percentage of Population Unable to Enroll

Because all biometric identification is based upon a physical characteristic of an individual, there will inevitably be a percentage of the population which cannot enroll in a particular biometric system. While there may be a greater percentage of the population able to use a fingerprint since the average person has at least 10 fingers, any biometric system will have a small population of users unable to enroll due to lack of the identifier

or a low-quality identifier. Regarding fingerprints, it is estimated that between 1% and 3% of the world's population would be unable to reliably use a fingerprint biometric system. [3]

### 2.3.7 Further Human Factors Considerations

It is not clear whether or not the effect human factors play is significant enough to greatly affect the overall accuracy of biometric systems. It is likely, however, that the degree to which human factors affect accuracy depends on the particular type of sensor used. A definitive study focused on the degree to which certain factors have effects on different sensor types could help determine quantify the degree to which human factors may or may not play a role. These issues are beyond the scope of this thesis and are not addressed, nor are they considered to be as significant as the social issues pertaining to the technology.

## 2.4 Technical and Implementation Issues

It is important to understand how biometric fingerprint systems compare to other types of biometrics in terms of accuracy, cost, and ease of use. As compared to other forms of biometric technologies, fingerprint biometric technology definitely holds many advantages. According to approximated figures given by a number of experts, fingerprint biometrics are superior to other common biometrics in terms of imaging, matching, and technology properties. A figure given by a number of experts in the biometric field rated fingerprint biometrics as having better matching properties when compared to other

major types of biometrics, including face, voice, and hand. [4] Table 2.1 shows the approximations used.

**Table 2.1:** Drawbacks of various biometric technologies [4]

Biometric Drawbacks	Finger	Face	Voice	Iris	Hand	Signature
<i>Intrinsic Properties</i>						
Cooperation required	High	Low	Low	Medium	High	High
Social stigma	High	Low	Low	Medium	Medium	Low
Intrusiveness	Medium	Low	Low	Medium	Medium	Low
Population Missing	Low	Low	Medium	Low	Medium	Medium
<i>Imaging Properties</i>						
Inconvenience	Low	Low	Low	Medium	Medium	Medium
Proximity required	High	Low	Low	Medium	High	High
Acquisition Time	Low	Low	Medium	Medium	Medium	Medium
Failure to Enroll	Medium	Low	Medium	High	Low	Low
Failure to image	Medium	Medium	Medium	Medium	Low	Low
<i>1:1 Matching Properties</i>						
#FA per 10K(FRR-10%)	0.1	10	300	0.001	10	300
#FA per 10K(FRR-1%)	10	1000	1000	0.1	100	1000
Template size (bytes)	500	1000	3000	250	100	200
<i>Technology Properties</i>						
Installation Cost	Low	Low	Low	Medium	Medium	Medium
Continual run cost	Low	Low	Low	Medium	Low	Low
Cost per match	Medium	Low	Low	Low	Medium	Low

#### 2.4.1 Fingerprint Biometric Performance

One of the most recent comparative and competitive test competitions for fingerprint technology was documented in March 2002. This competition, known as FVC2000, attempted to establish a common benchmark to allow for performance and improvements to be tracked. This competition shows that the best and worse case error rates for fingerprint identification are FRR of 3-7% and an FAR of 0.001-0.01%. Speed was another benchmark measured in the competition, with some systems able to enroll and identify fingerprints as quickly as 1 microsecond. [24] When compared to competitions for other biometrics, fingerprint identification has a superior FAR and FRR. Specifically, when compared to face, voice, iris, hand, and signature biometrics evaluated

through scenarios and technology evaluations, fingerprint biometrics has one of the lowest FAR rate, and one of the lowest FRR. [4] Table 2.2 shows a summary of the data.

**Table 2.2:** Error rates summarized from scenario and technology evaluations [4]

	FRR	FAR	Evaluation Method
Fingerprint	3-7%	0.001-0.01%	Technology Evaluation
Face	10-20%	0.1-1%	Technology and Scenario Evaluations
Voice	10-20%	2-5%	Technology Evaluation
Iris	2-10%	$\geq 0.001\%$	Scenario Evaluations
Hand	1-2%	1-2%	Scenario and Technology Evaluations
Signature	10-20%	2-5%	Technology and Scenario Evaluations

Another notable source of fingerprint biometric technology accuracy is from the Fingerprint Vendor Technology Evaluation 2003 (FpVTE), a test conducted by the NIST to fulfill part of its Patriot Act mandate. Thirty-four systems from 18 companies were tested using various subtests to measure accuracy for various types and numbers of fingerprints. The most accurate system tested using operational quality single fingerprints had between a 99.4% true accept rate @ 0.01% FAR and 99.9% true accept rate @ 1.00% FAR. [26]

#### 2.4.2 History of Fingerprint Usage

Because fingerprinting is among the oldest of biometric technologies available, it is also one of the most researched and well-known. Fingerprints were used as personal signatures around 300 B.C. in parts of Asia. Since the 1800s, fingerprints have been collected using ink and paper techniques in America. [3] In terms of maturity, fingerprint biometric technology is the most mature of all biometric technologies. [4] Fingerprint biometric technology has existed in early forms since the early 1970s, and was used by

the FBI to capture, store, and search fingerprint records since the late 1970s. [22] Because fingerprint technology is so well-known, there is a lot of information available on how to fool the technology into falsely accepting an invalid user. Documentation is available on how to create spoofed fingerprints to fool biometric scanners, and is noted later in this review of literature. [1] While it is possible to fool fingerprint scanners, it is difficult to accomplish.

#### 2.4.3 Fingerprint Biometric Cost and Availability

In terms of cost and availability, fingerprint sensors are one of the least expensive and most readily-available devices. Iris, hand, and signature scanners range in cost from \$300 to \$500 each. [4] Fingerprint scanners can be found for as little as \$25 on the Internet and can be purchased even cheaper in bulk. [21] Most big name retail outlets and online-retailers offer a variety of fingerprint scanning devices more so than other biometric devices. A large number of existing fingerprint templates available for public testing and other use exist online. The NIST has publicly available on its databases thousands of fingerprints in downloadable formats. [19] There are many companies which offer fingerprint biometric devices and systems, and there are many existing applications capable of using fingerprint biometrics. [1]

#### 2.4.4 Convenience of Fingerprint Biometrics

An estimated 40% of all help desk calls deal with password-related problems. [1] Because a user does not need to memorize their own biometric information, calls relating to password problems are rendered obsolete by utilizing fingerprint biometric technology. This would save help desk personnel time and consequently save the company large



amounts of money in the long run. Additionally, a fingerprint cannot be forgotten and is unlikely to be seriously damaged beyond recognition. Using a fingerprint scanner is much less intrusive than other biometrics, such as signature, iris, and retina biometrics.

#### 2.4.5 Implementation Issues

Proper implementation and education is critical in gaining user acceptance of a biometric system, and suggestions concerning this have been given in Julian Ashbourn's book Practical Biometrics: From Aspiration to Implementation. Because fingerprint biometric technology would be new in most organizations, a certain level of training is required for the administrative personnel of the system. Training would include the use of fingerprint biometric technology and the part operators play in the normal operation of the system. Personnel should be trained by the time the system is implemented, requiring an understanding of the underlying details of the system. [2] The training should consist of a general overview of the science of biometrics and detailed information including the fingerprint template creation process, storage of the biometric data, how to best use the system, and how to overcome any potential errors. Obtaining the optimal fingerprint sample from an individual needs to be taught to the staff administering the system. The individual tasks performed by the administrative staff also need to be addressed as part of the training process. Technical expertise should be taught at some level to the staff so that they will be able to differentiate between user error and system malfunctions. Distinguishing between spoofing attempts and genuine user error also needs to be taught to the staff. [2] Because users of the system will likely have questions or concerns, the staff should be capable of explaining the process to others at the conclusion of the training.

#### 2.4.5.1 User Training and Education

Part of any fingerprint biometric authentication system implementation is user training and education. The best way to overcome a user's negative preconceived notions of a system is good communication. The user's concerns need to be addressed and the system's use and benefits need to be enumerated. [2] Without acceptable training for the users of a system, the system may become burdensome to the users and create numerous problems for the system's administrative staff. A user with confidence in the process of interfacing with a fingerprint biometric system is likely to have less problems with the system than a user who is not confident. Training is best accomplished by means of education and specific training. [2] Education is important so that users understand the intention of the system, why it is used, and the part they will play in the enrollment/verification process. The process of communicating the intention of the system should be done in a clear, attractive, and informative manner. By doing so, users' confidence in the system will be increased and any lingering concerns will be alleviated. [2] The level to which confidence in a system could be increased by using education has not been closely measured. Such education could be a major factor in gaining user acceptance and overcoming false perceptions of fingerprint biometrics. Once the intentions of the system have been expressed to the user base, the enrollment process can be taught. This should give an overview of how the enrollment process works and should enumerate the steps required by the user to get their fingerprint enrolled in the system. After the users have been adequately educated as to the enrollment process, training should be carried out sufficient to meet the user's needs and should include the initial user enrollment. Once proper identification to validate individuals' identity is gathered, users can be enrolled. After successfully enrolling in the system, a few test transactions

should be made to test the enrollment of the user's biometric data. A reminder flyer could be issued to the user reminding them how to use the system and possibly reiterating the intentions of the system. While the education and training process may require a lot of materials, it needs to be done to ensure the users are adequately informed about the intentions of the system, how the system operates, and how the users use the system. In the long run, problems and potential errors are more likely to be avoided early on by following this process as opposed to overcoming problems later. [2]

#### 2.4.5.2 Enrollment Process

Though the intent of this thesis is not to describe or recommend a particular enrollment procedure wherein a specific individual's fingerprint is digitally registered, such a process is still critical in establishing a viable fingerprint biometric system. The enrollment process is meant to bind biometric identifiers with a described identity for a specific person. Verifying the identity of an individual during enrollment is paramount and must be done securely and in accordance with an established best-practice process. A biometric identity must uniquely specify and be linked with an individual's verified personal identity. If validating a claimed identity is done poorly, a false identity could be used for identity theft purposes or be linked to an individual with a criminal history.

Once an identity has been properly verified and a valid enrollment has been concluded, biometric data with a specific margin of error must be extracted from the captured fingerprint. Multiple images are often required in a fingerprint biometric system in order to get a usable template, and the number of images required varies from system to system. The uniqueness of a biometric fingerprint record is closely related to the amount of data and number of parameters extracted. Just as a computer screen with a

higher resolution displays greater detail and clarity, more data in the form of biometric parameters will produce a more unique personal biometric template. The degree of uniqueness of biometric templates should be tested to be in compliance with established security best practices during the initial user training and enrollment process by a system administrator. [2]

#### 2.4.5.3 Sensor Placement

Sensor placement with respect to the environment is an issue to consider in order for a system to operate consistently and reliably. Physical access to the fingerprint scanning device should be controlled to increase security. [1] An optimal location consists of an area in which temperature, humidity, light, and other environmental issues can be maintained and controlled to reduce the chances of sensor malfunction. [2] Regular maintenance should be performed to ensure that any built-up dirt and residue is removed from the sensor to maintain the accuracy of the system. [1]

### 2.5 Security Issues

Biometric identification is not perfect in terms of security, nor is any other identity management technology. Irregardless of the system, any biometric system eventually will statistically allow unwanted individuals to be authenticated. No system is entirely free from attack by intruder when accounting for the various possibilities of attack on biometric fingerprint systems. [4]

### 2.5.1 Points of Vulnerability

In most biometric systems, there are approximately eight possible points of attack. For system administrators, these points of attack are important to understand in order to avoid problems and intruders. These points of attack are (1) at the biometric sensor, (2) between the sensor and the biometric system, (3) at the biometric feature extractor, (4) between the feature extraction process and matching process within the biometric system, (5) within the matcher itself, (6) at the output of the matcher, (7) between the template database and the biometric system, and (8) within the database of stored templates. [4]

The first point of attack is usually exploited by using a falsified fingerprint taken from a legitimate user. Existing methods of fingerprint ‘spoofing’ are discussed later on. The second point of attack is exploited by resubmitting the digital capture of a previously recorded fingerprint to the feature extractor. At the third point of attack, the feature extractor is bypassed or attacked to pass on false data to the matching system. The fourth point of attack would be exploited by tampering with the raw fingerprint feature data and replacing it with stolen data from a valid user’s fingerprint. The matcher itself, the fifth point of attack, can be altered so that it creates a desired match score, which could potentially validate an invalid user. The output of the matcher, attack point six, could be overridden to classify an illegitimate user as legitimate. Point seven could be attacked by modifying the communications link between the database and the biometric software to falsify the data from the database, causing the system to make a misinformed decision. Finally, the existing data within the database itself could be modified or new template information could be inserted causing an intruder to be stored in the database as a valid user.

Attacks at points 2 through 8 require a working knowledge of computers, data communication in computer systems, and access to the biometric system itself. Therefore, the most likely and common point of attack is at the sensor itself. An attack where a legitimate user's biometric data is presented by an intruder is known as a coercive attack [4] and is also known as "spoofing". While this could potentially be accomplished by physically removing a biometric identifier from a legitimate user, a simpler and more likely approach is to copy a latent fingerprint and use it to authenticate an unauthorized user as an authorized one.

### 2.5.2 Vulnerability Studies

Many different studies have been previously performed which show the vulnerability of fingerprint biometric systems. A study published by Putte and Keuning [11] involved creating false fingerprints using silicone rubber. One method required a valid user's cooperation to obtain the plastic cast of the original finger. The majority of the fingerprint sensors tested in the study allowed the false fingerprint to be validated as a genuine user. Their study also included creating a silicone finger using a latent fingerprint, a method which does not require a user's cooperation but does require effort to find a usable latent fingerprint. In the study, the latent fingerprint is dusted with an extremely fine powder, transferred, and photographed for projection to a printed circuit board. By using a combination of acid and ultraviolet radiation, a duplicate of the print is etched on the board. The print etched on the board is then used to create a silicone duplicate print from easily accessible and inexpensive materials. Out of the six sensors tested by the authors, five of them accepted the false print as genuine.

### 2.5.3 Liveness Detection

Legitimate fingerprints can be determined by using sensors which sense electrical activity, temperature, and pulse in fingers. [4] Some of the properties used by fingerprint scanner manufactures for differentiating between live and spoofed fingers include heartbeat, heat, temperature, and conductivity. Often, these liveness-detection methods cannot perform well because of different environmental conditions. The thinness of spoofed fingerprints may or may not be detected by sensors. [11] What happens when a fingerprint is stolen? Multiple fingerprints can and should be used in this situation, and the pattern of them should be changed from time to time. [1] Technology is being improved upon constantly in order to increase overall security, accuracy and reliability of fingerprint scanners. [2]

## 2.6 Summary

While much has been written and studied with regard to fingerprint biometric technology, no definitive study focusing directly on fingerprint biometric technology and the social reasons for its lack of proliferation throughout society and commerce could be identified. The studies and publications noted in this review of literature show the need for the additional research conducted in this thesis and give an excellent basis for the research conducted in this thesis. The proceeding chapters detail the research method used in this study and draw conclusions from the resulting data.

## CHAPTER 3 – RESEARCH METHODOLOGY

### 3.1 Introduction

To better determine the effects of societal factors and user perceptions upon the utilization of fingerprint biometric technology, a number of research methods were employed. The research in this study consisted of four phases enlisting distinctive methods, as explained below.

#### 3.1.1 Introduction of Phase I

The first phase was to better understand fingerprint biometric technology by creating a process whereby fingerprint minutiae were extracted from a sample fingerprint image taken from a fingerprint scanner. The purpose of this was two-fold: (1) for the benefit of the researcher's understanding and technical background regarding fingerprint biometric technology, and (2) to use as a technical demonstration of fingerprint biometric technology to facilitate the understanding by a basically illiterate and biased sample population. This was important in order to demonstrate to users that fingerprint biometric systems do not use actual fingerprint images to perform matching functions; these systems use data parameters that represent features of the fingerprint.



### 3.1.2 Introduction of Phase II

The second phase of the research was to create and administer an interview-style survey to determine the perceptions of the population regarding fingerprint biometrics. A portion of the individuals surveyed were shown how fingerprint scanners work and, additionally, were shown the feature extraction process created from Phase I of the research. The other portion was only interviewed without having received the technical demonstration. This was another variable, aside from demographic variables, used in this phase of the research and was used to quantify the level to which an informative technical demonstration influences the perceptions of individuals. Questions were focused on the potential false perceptions and concerns arising from implementation of the technology, mainly those problems highlighted in the literature review. Demographic information obtained in this phase of the research was used to validate the demographic variation of individuals responding to the survey questions. Though much of this demographic information was used in further analyzing responses to the questions, this was not the primary purpose of the demographic data.

### 3.1.3 Introduction of Phase III

The third part of the research involved creating a brief informational document outlining the facts concerning fingerprint biometric technology and sharing it with individuals. The facts directly addressed pre-identified potential concerns with the technology and sought to alleviate those concerns. These individuals were asked to fill out an online survey to measure the extent to which this brief education might have reassured them as to the viability and security of fingerprint biometric technology. The survey closely mirrored the survey in Phase II for the purpose of comparing the degree to

which any responses to the questions had changed after having received the facts of the technology. Little demographic information was obtained in this phase of the research since studying the effect of varying demographics on responses was not an objective. Therefore, most of the demographic variables are not considered in the analysis of this data. Additionally, it was anticipated that some respondents would be less willing to participate in the online portion if personal information such as age were requested, and users may have rated their technical expertise differently between the two surveys.

#### 3.1.4 Introduction of Phase IV

The main focus of the fourth phase of the research was to gain an authoritative opinion of identity management technology usage by interviewing key authorities involved in Utah's abortive 1997 legislation that proposed using smart card technology in the driver's license issuance process. The author wanted to better understand the political reasons for its defeat. The authorities contacted were Utah State Legislators involved in the 1997 Smart Card Drivers License legislation. Their opinions and reasoning for accepting or rejecting smart card technology in driver's licenses gives a clearer picture of the potential widespread acceptance, or lack thereof, of fingerprint biometric technology in public settings. Because both smart-card and biometric technology are controversial identity-management technologies, the authoritative opinions gathered were of great value to this research.

## 3.2 Phase I

An important part of the research was to choose hardware and software able to extract and display the electronic data representing features of scanned fingerprints. This phase of the research was important for two reasons: (1) to further the researcher's background and understanding of the technology, and (2) because a portion of the population in Phase II were shown a demo of the technology along with the feature extraction process to help facilitate understanding and illustrate to users that fingerprint features are used rather than full-images.

### 3.2.1 Locating Necessary Hardware and Software

A fingerprint scanner was readily available through Brigham Young University's IT department. The scanner used was a Targus Defcon 1 Authenticator model number PA460, using an AuthenTec EntréPad™ AES4000 fingerprint sensor, shown below in Figure 3.1. This is a common sensor used in many manufacturers' fingerprint scanners.



**Figure 3.1:** Targus Defcon biometric authenticator

There was no software bundled with the scanner to view the data extracted from fingerprints. After contacting AuthenTec for further information about their software, a copy of their SDK was received. The SDK contains the AuthenTec Windows Fingerprint Software API, a comprehensive set of functions for supporting applications using one or more Defcon Authenticators and included a number of basic software applications for capturing fingerprint images, and sample applications used for identifying users based on fingerprints. The applications illustrate the AWFS API's usage and provide examples of how it can be used. Effective as it is, raw data cannot be obtained and viewed using their SDK. Proprietary methods of feature extraction, template creation, template matching, and data storage are utilized by AuthenTec. For privacy reasons, the company was not willing to allow outsiders access to the algorithms or extraction methods used in their systems and databases. Therefore, another method of extracting fingerprint data needed to be discovered.

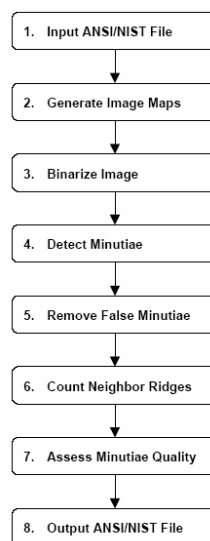
#### 3.2.1.1 NIST Public Domain Fingerprint Software

Open-source fingerprint extraction software is uncommon in the public-domain. The only known organization with freely available software capable of extracting and displaying fingerprint data using an open standard is the National Institute of Standards and Technology. The NIST is a non-regulatory federal agency part of the U.S. Commerce Department's Technology Administration which develops and promotes standards to facilitate processes. Their standard for fingerprint information extraction is known as the ANSI.NIST-ITL 1-2000, also known as the NIST Data Format for the Interface of Fingerprint, Facial, & Scar Mask & Tattoo (SMT) Information. A software package available from the NIST, known as MINDTCT is a fingerprint minutiae detector

which is capable of locating bifurcations and ridge endings in fingerprint images. This software is used by the Federal Bureau of Investigation in their ‘Universal Latent Workstation’. The software uses the NIST’s “Data Format for the Interchange of Fingerprint, Facial, Scar Mark & Tattoo (SMT) Information” standard, also known as ANSI/NIST-ITL 1-2000. The public domain software available from them includes a fingerprint categorization program called PCASYS, minutiae detection software called MINDTCT, a data formatting software suite called AN2K, and image transformation utilities. The central piece of software needed in this case for extracting fingerprint data is MINDTCT.

### 3.2.1.2 MINDTCT

MINDTCT is minutiae detection software which automatically locates and records ridge endings and bifurcations in a fingerprint image. The minutiae quality assessment is also done and is based on local image conditions. MINDTCT is used by the FBI in their Universal Latent Workstation and is the only known public domain system of its kind.



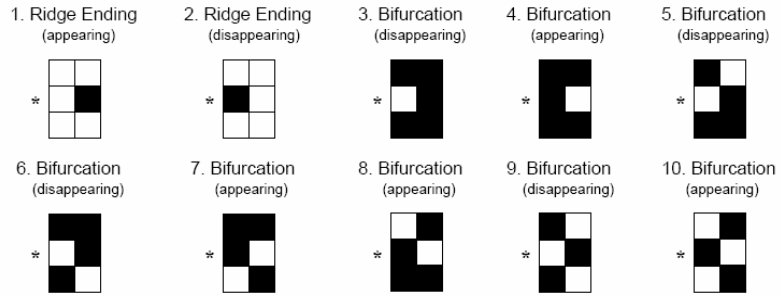
**Figure 3.2:** NIST’s MINDTCT minutiae detection process [22]

Figure 3.2 shows the process by which MINDTCT operates on a file to extract the fingerprint's minutiae. MINDTCT requires an ANSI/NIST-formatted file as its input. A portion of this file format is seen in Figure 3.6. Once the ANSI/NIST file is created, an image map is generated from the file, and the image is binarized so ridges and valleys can be differentiated. An example of binarization is shown in Figure 3.3 below.



**Figure 3.3:** Fingerprint image before binarization (left) and after binarization (right) [22]

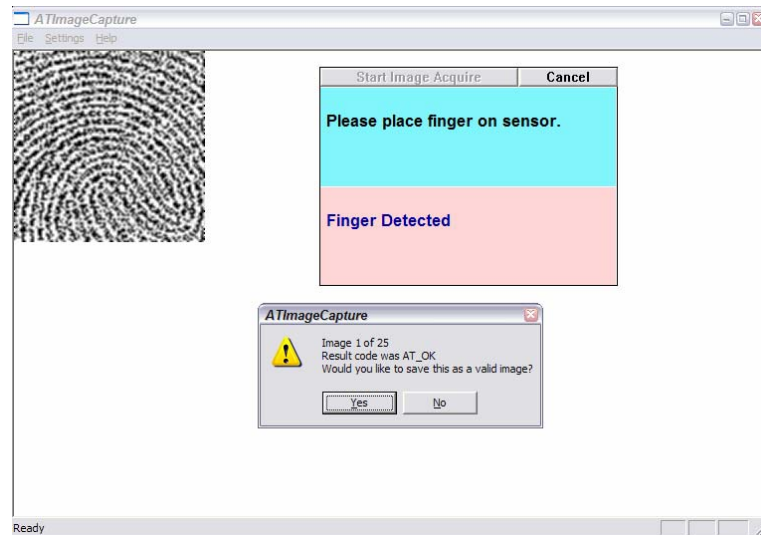
Once binarized, the fingerprint minutiae can be detected. Figure 3.4 below shows the pixel patterns used to detect minutiae. The minutiae fall into one of four categories, appearing bifurcation, disappearing bifurcation, appearing ridge ending, and disappearing ridge ending. After the minutiae are detected, false minutiae are removed using special filtering algorithms. The number of ridges between each neighboring minutiae are counted—a parameter often used by fingerprint matchers. The quality of each minutiae is calculated and a resulting ANSI/NIST file along with a text file detailing the minutiae information. The format of this outputted text file is discussed in further detail in Chapter 4.



**Figure 3.4:** Pixel patterns used to detect minutiae

### 3.2.2 Converting Scanned Image to NIST's AN2K Format

Though challenging as it was to extract fingerprint data from a scanned fingerprint image, it was possible using the Targus Defcon Authenticator and accompanying SDK software. ATImageCapture is included as a small program for capturing images from the sensor, shown in Figure 3.5. The simple program waits for the detection of a finger on the sensor and captures an image of the finger, and while it operated with minimal intervention, it often crashed and needed to be restarted.



**Figure 3.5:** ATImageCapture software screen capture

ATImageCapture allows for various sizes of images to be captured, from 250 dpi to 1000 dpi. For this process, 500 dpi is used as a nominal image size. Each image was automatically saved to the root directory as a bitmap image with the default name 'TestUser7vXXX.bmp'. This image type was not acceptable as is for MINDTCT which requires an AN2K-formatted file and raw image data as input. Therefore, the bitmap file needed to be converted to RAW format and was done using the freeware tool, BMP2RAW.

### 3.2.2.1 Type-14 Variable-Resolution Record Layout

Once the image was converted, the input AN2K file was created using the NIST tool called TXT2AN2K. TXT2AN2K accepts as a parameter a formatted text file which is read and converted to conform to the ANSI/NIST-ITL 1-2000 standard. For this process, the type-14 variable-resolution record layout for fingerprint image data was used. Table 3.1 shows the layout for this record type. Field 14.001, logical record length, was needed but can be entered as an arbitrary number since TXT2AN2K is smart enough to replace the value with the correct length at conversion time. The next four fields, 14.002-14.005 are not critical for file conversion, but are important for agencies like the FBI who need to have meta-data about each fingerprint recorded. The number of pixels horizontally and vertically was used as the sixth and seventh fields, 14.006 and 14.007. The scale units field, 14.008, requires a '1' in this case to specify pixels per inch. The next two fields, 14.009 and 14.010 require the pixel density of the image used, so if there were 192 pixels in one direction and pixels per inch were specified, 96 would be the pixel density of the image on a two-inch wide image. When using the RAW image format, no compression algorithm was used, so field 14.011 was left blank. The number



of bits per pixel, usually eight, was inputted in field 14.012. The remaining fields, 14.013 to 14.998 can be arbitrarily filled, except for the image data field 14.999 which contains the filename of the RAW-formatted image file.

After formatting the text file, TXT2AN2K runs with the text file as its first argument, and the name of the outputted an2k file as the second. After converting the text file, the minutiae are extracted using MINDTCT. The resulting text file can be viewed to see the minutiae information.

**Table 3.1:** Type-14 variable-resolution tenprint record layout [28]

**Type-14 variable-resolution tenprint record layout**

Ident	Cond code	Field number	Field name	Char type	Field size per occurrence		Occur count		Max byte count
					min	max	min	Max	
LEN	M	14.001	LOGICAL RECORD LENGTH	N	4	8	1	1	15
IDC	M	14.002	IMAGE DESIGNATION CHARACTER	N	2	5	1	1	12
IMP	M	14.003	IMPRESSION TYPE	A	2	2	1	1	9
SRC	M	14.004	SOURCE AGENCY / ORI	AN	10	21	1	1	28
TCD	M	14.005	TENPRINT CAPTURE DATE	N	9	9	1	1	16
HLL	M	14.006	HORIZONTAL LINE LENGTH	N	4	5	1	1	12
VLL	M	14.007	VERTICAL LINE LENGTH	N	4	5	1	1	12
SLC	M	14.008	SCALE UNITS	N	2	2	1	1	9
HPS	M	14.009	HORIZONTAL PIXEL SCALE	N	2	5	1	1	12
VPS	M	14.010	VERTICAL PIXEL SCALE	N	2	5	1	1	12
CGA	M	14.011	COMPRESSION ALGORITHM	A	5	7	1	1	14
BPX	M	14.012	BITS PER PIXEL	N	2	3	1	1	10
FGP	M	14.013	FINGER POSITION	N	2	3	1	6	25
RSV		14.014 14.019	RESERVED FOR FUTURE DEFINITION	--	--	--	--	--	--
COM	O	14.020	COMMENT	A	2	128	0	1	128
RSV		14.021 14.199	RESERVED FOR FUTURE DEFINITION	--	--	--	--	--	--
UDF	O	14.200 14.998	USER-DEFINED FIELDS	--	--	--	--	--	--
DAT	M	14.999	IMAGE DATA	B	2	--	1	1	--

Key for character type: N = Numeric; A = Alphabetic; AN = Alphanumeric; B = Binary

Figure 3.6 illustrates features and feature direction markers transposed over a fingerprint image. Chapter 4 shows how the entire process was automated and the resulting information extracted from a sample fingerprint. The process described above for

extracting minutiae was shown to some of the participants of Phase II of the research to facilitate their understanding of how fingerprint features are extracted and used for unique identification.



**Figure 3.6:** Minutiae and direction superimposed over a fingerprint image

### 3.3 Phase II

The second part of the research was to create and administer an interview-style survey to determine the feelings of the population regarding fingerprint biometrics. A portion of the individuals surveyed were shown how fingerprint scanners work and shown the feature extraction process determined from the first part of the research. Others were only interviewed without having received the technical demonstration. This helped quantify the level to which a technical demonstration influences the opinion of individuals. Other factors taken into account were demographic factors such as age, sex, and education level. Occupation and technical expertise were also considered significant and were considered in the analysis of the results.

### 3.3.1 Sample Population

The level to which the social issues and user perceptions discussed in the previous chapter exist among a targeted population was investigated using interview-style surveys from the population. The sample population demographic consisted of individuals with varying levels of technical expertise and education between the ages of 18 and 65 and living in the Salt Lake and Utah County areas. Demographic information including age, sex, technical expertise, and occupation were gathered to ensure a varied population. The majority of the targeted population work in large organizations where fingerprint biometric technology is not used, but could be applicable, and employees were of varying job types and technical expertise. The main areas targeted were technical, education, and state/federal agencies in the state of Utah. These organizations were those which are recognized, well-known in the Salt Lake and Utah County area and easily accessible by the researcher, namely Novell Inc., Brigham Young University, and the Utah State Parks and Recreation. Aside from these targeted individuals, an additional random population was sampled, chosen randomly by undergraduate students assisting in the research from among the general population of the Salt Lake and Utah County areas and comprising various backgrounds.

#### 3.3.1.1 Appropriateness of Population Selection

This sample population was determined to be appropriate for the following reasons:

(1) the majority of working adults in Utah is between the ages of 18 and 65 and thus would be able to use a fingerprint biometric scanner in a public setting.

(2) Both technically-oriented and non-technically oriented individuals make up the general population and may offer different opinions as to the validity of fingerprint biometric technology.

(3) Technical, educational, and state/federal agencies all work with private information and likely would have valid and useful opinions on biometric technology.

(4) Because this study was limited to a relatively small geographical area, the organizations chosen were well-known and representative of various, major industries within the state.

(5) The legislative population has had direct experience in debating and voting on identity management technologies such as smart cards and would offer useful insight as to the future validity and acceptability of biometric technology on a wide scale.

#### 3.3.1.2 Random Sampling

All of the participants of this study were chosen randomly, but were mostly targeted from specific organizations. From Novell, participants were located on various levels in different buildings of the Provo, Utah campus. Over 30 individuals were selected from around the company to participate randomly, simply by knocking on office doors around the company on different days, resulting in a population with varying demographics, levels of technical expertise, and exposure to biometric technology. From Brigham Young University, participants were again chosen at random and among the faculty and staff of the Marriott School of Management, School of Technology, and various other departments within the organization, comprising over 40 participants of this study. From the State of Utah, participants were chosen at random from among the main campus of the Utah Department of Parks and Recreation in Salt Lake City, Utah. This

particular campus was chosen because of the diverse backgrounds of employees, ranging from park rangers to information technology specialists, and the varying level of technical expertise among the population. Roughly 30 participants were located and chosen to participate in the survey from this area. The remaining participants were selected randomly by a group of undergraduate students commissioned to distribute the survey to 10 random individuals of their choosing. The resulting participants were of varying age, ethnicity, sex, technical expertise, and occupation.

The samples taken in this study may not be representative of the general population of the United States, nor even of the entire state of Utah, since the majority of the participants live in the Salt Lake and Utah County area. However, the samples can be considered representative of government, education, and technology sectors in the northern Utah area. The majority of the sample population was well-educated, living in areas of little criminal activity, and trusting of others. Utah ranks among the leading states in educational attainment of its population. In the year 2000, 90.7% of Utahns over the age of 35 completed high school, and roughly 26.9% had earned a bachelor's degree or higher. As of 2003, Utah ranked second in the nation for higher education spending and also ranks second in the nation for percentage of households with computers. [29] Because Utah appears to be better educated than many other states in the nation, more accurate and thoughtful responses may have been offered than those which could have been obtained outside the state.

### 3.3.1.3 Sample Size

The population selected consists of individuals from education, technology, and government organizations which are significant within the Salt Lake and Utah county

area. Novell, Brigham Young University, and Utah State Parks and Recreation offices were selected due to their large size, diverse staff, and the applicability of the technology. The required sample population size was calculated using the following sample size formula:

$$ss = \frac{Z^2 * (p) * (1-p)}{c^2}$$

The total required sample size was calculated using a 95% confidence interval (Z=1.96), a p value of 0.5, and a confidence interval (c) of ±8%. By entering these values in the formula, the total required sample size (ss) was at least 150 individuals to be sampled. 170 total individuals were surveyed, an excess of 20 individuals.

#### 3.3.1.4 Involvement of Survey Experts

The questions used in this survey were shown to a number of professionals in the field of surveying at Brigham Young University, including survey specialist Michael D. Geurts of the Marriott School of Management at BYU, and Mark D. Allen and Bruce Brown, psychology professors at BYU. They reviewed initial drafts of the questions and offered suggestions to help make the survey questions less biased and more effective.

#### 3.3.2 Survey Questions

The survey played a dual role: 1) to identify what concerns the target population had regarding fingerprint biometric technology and 2) to determine the level to which certain concerns and perceptions exist. All questions, aside from questions 1, 4, 5 and 18, used a 7-point Likert scale to allow for a more quantifiable and detailed analysis of responses.

*Question 1: How many times have you been a victim of identity theft?*

This question was intended to determine if an individual had ever experienced a serious invasion of privacy resulting in identity theft. If an individual had been a victim of identity theft, he may be more hesitant about using fingerprint technology due to a perceived risk of having his fingerprint stolen compared to an individual who has not been a victim.

*Question 2: To what degree do you consider security more important than convenience?*

This question was meant to gauge the level to which general security was an issue for the surveyed population. Because there is a tradeoff between the level of security and the level of convenience of most systems and this could affect an implementation of a fingerprint biometric system, it was important to measure the population's opinions about this tradeoff and its affect on responses to other questions.

*Question 3: How familiar are you with biometrics in general?*

Individuals familiar with biometric technology are more likely to have a greater factual-base for how it operates. The study sought individuals with little or no experience with biometrics since the majority of the population was not likely to be familiar with the technology. Individuals who are familiar with the technology were also welcome and important to the study, but it was assumed that their knowledge would result in different responses to the proceeding questions.

*Question 4: How many times have you used a fingerprint biometric reader?*

Similar to the previous question, it sought to determine if individuals had any previous experience with fingerprint scanners. Those with previous experience would be less likely to have misconceptions about the technology. It was assumed that different insight could be gained by those who have had experience with the technology and they would have fewer concerns. The majority of individuals was assumed to have never used a biometric reader and could give responses more similar to those of the general population.

*Question 5: What concerns do you have about using your fingerprint for identification purposes?*

This open-ended question was meant to determine the initial perceptions and thoughts of respondents about any concerns they may have had about fingerprint usage. This question was asked to discover any initial concerns and perceptions regarding the technology prior to responding to the proceeding questions.

*Question 6: To what degree would you consider fingerprint scanning an invasion of your personal privacy?*

This question sought to measure the degree to which fingerprint scanning was perceived as a privacy invasion by the surveyed population. It was asked because of the amount of privacy-related issues mentioned in current literature regarding the technology, and thus was a likely concern among the population. Privacy concerns are a critical part of any identity management system and are especially important to understand with fingerprint biometric systems.



*Question 7: How easy do you think it is for fingerprints to be stolen or copied?*

It was important to find out the degree to which the population believes fingerprints can generally be stolen or copied. Many movies which portray fingerprint scanning show latent prints being stolen and reused by thieves to impersonate valid users. It was important to understand how easily the population believes fingerprints can be stolen or copied as it would suggest a major concern regarding the technology.

*Question 8: After using a fingerprint scanner in a public setting, how easy do you think it would be for your fingerprint information to be stolen or copied?*

This question addressed fingerprint scanner usage in public settings and the perception that fingerprint information can be stolen after using a public scanner. This question differs from the previous question because it specifically addresses public fingerprint scanner usage. It helped better illustrate the public's concern and perception of possible fingerprint theft from public fingerprint systems.

*Question 9: After using a fingerprint scanner in a public setting, how concerned would you be about your fingerprint information being distributed, shared, or accessed by a 3rd party?*

This question was similar to the previous question but seeks to establish the level of concern about the access, distribution, and sharing of fingerprints to third parties. Individuals may be concerned with information being given to other organizations for illegitimate purposes. The prevalence of this perception was important to establish since anyone believing their fingerprint data could be shared across systems or with other organizations would be very unlikely to accept the technology.

*Question 10: Suppose the organization you worked for enforced a policy of fingerprinting each employee. Can this organization legally require you to give your fingerprint?*

The perceived legality of obtaining fingerprints from individuals by administrative entities was sought by this question. Users may be reluctant or unwilling to use fingerprint scanners if they did not know their rights and the rights of the organization concerning fingerprint usage. Since this issue and perception is not concretely defined, the degree to which concerns over this area of the technology was important to establish.

*Question 11: Can a fingerprint image be reconstructed from raw biometric data?*

Security of biometric data was a concern mentioned in numerous literatures. A major security issue is the possibility of reconstructing a fingerprint pattern from the extracted fingerprint parameter data. A population with the perception that a fingerprint can be reconstructed from extracted fingerprint data would be uncomfortable using a fingerprint biometric system.

*Question 12: To what degree do you have religious or moral objections about using your fingerprint for identification?*

This question was asked because of known opposition to identity management technology by groups such as the Eagle Forum and other ultra-conservative organizations. It was expected that a minimal percentage of the sample population would have moral or religious objections. This concern was not something that could be alleviated through education or training, yet this perception among the sampled population was important to quantify.

*Question 13: To what degree would you consider using a fingerprint scanner hazardous to your health (i.e. pain, electrical shock, germs?)*

The level to which a health threat could be experienced through using a fingerprint scanner, while expected to be low, was still asked as to measure the level of concern. The question covers the majority of potential health threats, namely pain, germs, and electrical shock.

*Question 14: How accurate do you think fingerprint scanners are?*

The perceived accuracy of fingerprint scanners was important to determine. A population viewing fingerprint biometric scanners as inaccurate would be unlikely to accept the implementation. This question gave a measurement as to the perceived level of accuracy of fingerprint scanners in general.

*Question 15: How comfortable would you be with using your fingerprint to enter the building you work in?*

One of the most logical uses for fingerprint biometric technology is access to buildings and other restricted areas. Hence, this question was posed to measure how comfortable the population was with using a fingerprint for such a purpose.

*Question 16: To what degree would you consider a fingerprint more convenient than other security measures? (keycode, password, smart card)*

An important measure of the validity of identity management technologies is the overall convenience of the system. The perceived convenience of fingerprint biometrics was deemed important to determine. A population perceiving the technology as convenient would likely embrace it more willingly.

*Question 17: To what degree would you consider using a fingerprint more secure than other security measures? (keycode, password, smart card)*

Security is an important measure of any identity management technology, particularly fingerprint biometric technology. The level of perceived overall security of fingerprint biometrics compared to other basic identity management tools was deemed as important to determine. The level of security perceived in a fingerprint biometric system is directly related to the level of user acceptance of that system.

*Question 18: Of all the concerns about fingerprints mentioned (privacy, security, legality, morality, accuracy, health) what is your most significant concern with the technology?*

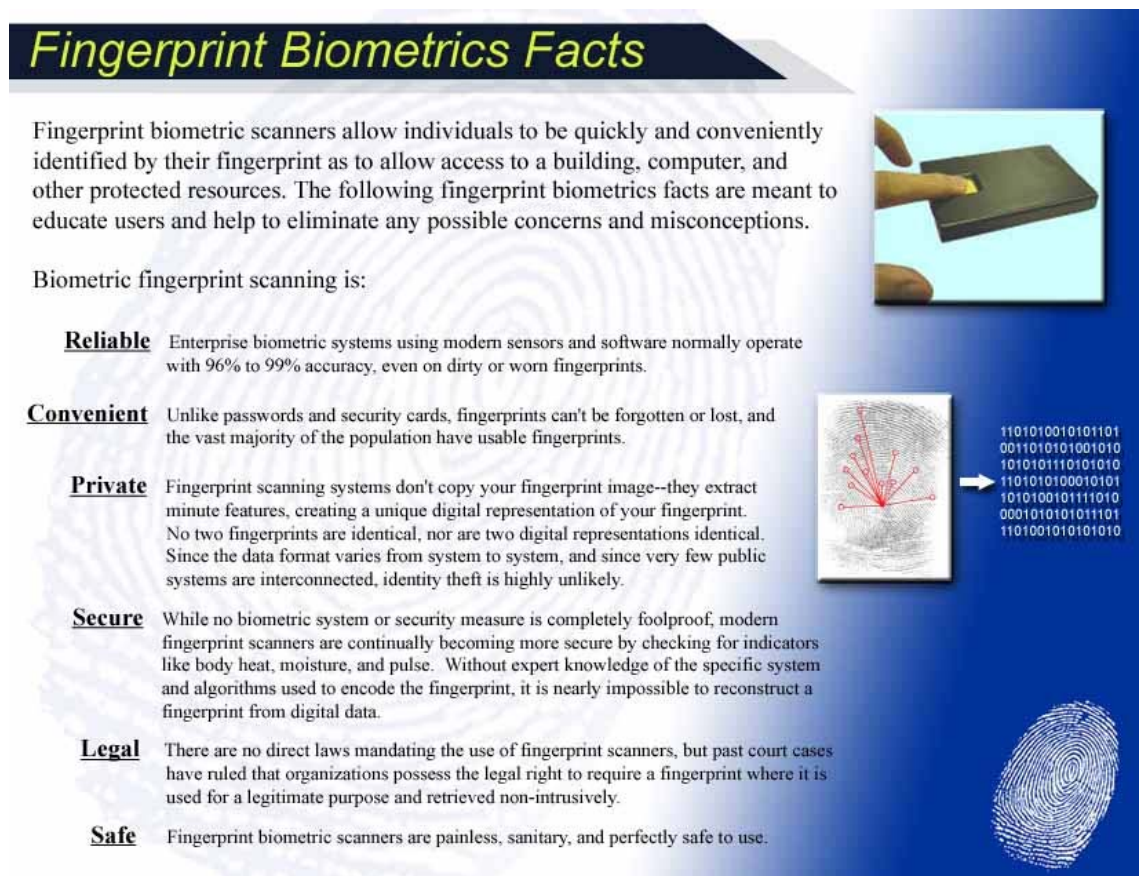
This final question seeks to identify the most paramount concern among the surveyed population. Though similar to question 5, it was asked at the end of the interview to determine if any of the preceding questions raised additional concerns among the population.

### 3.4 Phase III

The final phase of the research consisted of condensing scientifically-established facts regarding fingerprint biometrics and creating a web page with an overview of these facts. This phase was meant to test the hypothesis outlined in Chapter 1 by determining whether or not individuals who had received education regarding the facts of the technology exhibit a higher level of acceptance and understanding of fingerprint biometric technology than previously exhibited in the initial survey.

### 3.4.1 Technology Overview

The information compiled for this was gathered mostly from the literature reviewed in Chapter 2 of this thesis. It covered all of the major areas of possible concern about fingerprint biometric technology, namely: (1) reliability, (2) convenience, (3) privacy, (4) security, (5) legality, and (6) safety. The information was meant to communicate the reality of each of these areas and to help positively alter perceptions such that the technology would be more greatly embraced. This technology overview is shown in Figure 3.7.



**Fingerprint Biometrics Facts**

Fingerprint biometric scanners allow individuals to be quickly and conveniently identified by their fingerprint as to allow access to a building, computer, and other protected resources. The following fingerprint biometrics facts are meant to educate users and help to eliminate any possible concerns and misconceptions.

Biometric fingerprint scanning is:

- Reliable** Enterprise biometric systems using modern sensors and software normally operate with 96% to 99% accuracy, even on dirty or worn fingerprints.
- Convenient** Unlike passwords and security cards, fingerprints can't be forgotten or lost, and the vast majority of the population have usable fingerprints.
- Private** Fingerprint scanning systems don't copy your fingerprint image--they extract minute features, creating a unique digital representation of your fingerprint. No two fingerprints are identical, nor are two digital representations identical. Since the data format varies from system to system, and since very few public systems are interconnected, identity theft is highly unlikely.
- Secure** While no biometric system or security measure is completely foolproof, modern fingerprint scanners are continually becoming more secure by checking for indicators like body heat, moisture, and pulse. Without expert knowledge of the specific system and algorithms used to encode the fingerprint, it is nearly impossible to reconstruct a fingerprint from digital data.
- Legal** There are no direct laws mandating the use of fingerprint scanners, but past court cases have ruled that organizations possess the legal right to require a fingerprint where it is used for a legitimate purpose and retrieved non-intrusively.
- Safe** Fingerprint biometric scanners are painless, sanitary, and perfectly safe to use.

The infographic includes several visual elements: a hand scanning a fingerprint on a device, a diagram of a fingerprint with red lines indicating feature extraction, a binary code sequence, and a close-up of a fingerprint.

Figure 3.7: Facts of fingerprint biometric technology

### 3.4.2 Online Survey

Following the presentation of this overview, a brief survey was administered in an online forum. The majority of the questions contained in the survey were identical to those asked in Phase II of the research and used the same 7-point Likert scale as in the previous survey. The purpose of this was to establish the variation in responses between the two surveys stemming from the effect of education. The survey consisted of many of the same questions as the survey of Phase II, namely questions 6, 7, 8, 9, 10, 11, 13, 14, 15, 16, and 17. The differences in responses between the two surveys were measured to determine the variation in responses. Demographic information was not factored into the final analysis since its primary use was to validate the variation among the demographics represented in the Phase II survey. Also, demographic information including age, occupation, and names were not required to submit the survey since trepidation about submitting personal information online was anticipated. Therefore, analysis of these results by demographics was minimized. The main focus of this survey was to analyze the overall effects of the education on the entire surveyed population. Aside from the eleven questions from the original survey, four additional questions were asked to ascertain the perceived value of the biometric technology overview:

- *To what degree did the previous page reassure you about fingerprint biometrics in general?*

This question sought to quantify the degree to which respondents experienced reassurance as to the validity of fingerprint biometric technology in general due to the online technology overview. This helped quantify the level to which the information had effect on the population's opinion of the technology and whether they felt reassured and more willing to use the technology.

- *Having read the previous information, how willing would you be to use a public fingerprint scanner at your place of employment?*

This question quantified the degree to which individuals felt more willing to use a public fingerprint scanner in an employment setting after having read the fingerprint biometric technology overview. Since biometric fingerprint technology is applicable and has a logical use in places of employment for access to secure areas and resources, the responses to this question were significant.

- *Having read the previous information, how willing would you be to use a public fingerprint scanner at a commercial location?*

Similar to the previous question, this measured the level to which users would find biometric fingerprint scanning acceptable in a commercial setting after having read the educational facts of fingerprint biometrics. It was assumed that there would be a difference between user acceptance in a commercial setting compared to an employment setting for fingerprint biometrics.

- *To what degree did the previous page help you better understand how fingerprint scanners work?*

This question quantified the degree to which individuals better understood the operation of fingerprint scanners after having read the information on the technology. Individuals who understand the technology would be more likely to accept the technology and feel comfortable using it.

### 3.5 Phase IV

This phase of the research involved contacting Utah state legislators to gain an authoritative opinion on the 1997 legislation of a identity management system comparable to fingerprint biometric technology. The Utah House of Representatives was involved in Utah's February 1997 legislation process of determining whether or not smart card technology should be incorporated into Utah State Drivers Licenses. Though the bill passed the House of Representatives by a margin of 43 to 23, the bill only made it to the interim calendar of the Senate and was never revisited. The representatives contacted were those who had participated in the debates and voting. Their opinions and reasoning for either accepting or rejecting smart card technology in driver's licenses foreshadows of the potential widespread acceptance of a large-scale deployment of fingerprint biometric technology in the Utah area. Because both smart-card and biometric technology are controversial identity-management technologies, the authoritative opinions gathered were of great value to this research.

Because of the very busy schedules of the State House of Representatives, email was decided upon as the easiest and most efficient way of gathering information about the 1997 legislation. The questions selected for the legislators address the February 1997 smart-card technology driver's licenses legislation and the issues which arose among the Representatives and opposition groups. Specific information or explanation as to why the technology never made it into driver's licenses was determined to best be gathered from the representatives themselves. The next section shows the questions asked of the state representatives.



### 3.5.1 Questions Asked of Representatives

*Question 1: Were you a member of the legislature when the Smart Card topic was voted on? If so, how involved were you in the legislative process involving the use of driver's license smart cards?*

This question was used to make sure the contacted representatives played some role in either the debate or vote on smart card driver's licenses, and if so, to what degree the legislators were involved. Though a list of legislators who voted on the legislation exists on the Internet, it was important have assurance the legislator was involved in the process to some degree.

*Question 2: What issues prompted you to vote the way you did?*

This question was asked to determine the main issues regarding the legislation which prompted the representative to vote the way he did. These issues are significant and applicable to future fingerprint biometric legislation or large-scale implementation.

*Question 3: What factors allowed the vote to make it through the legislature?*

This question was meant to determine the factors which allowed the legislation to make it through the House of Representatives. Since the legislation was not pursued further, it was interesting to see why it made it through the House and was dropped by the Senate.

*Question 4: What groups prevented the legislation from being passed by the senate?*

This question was similar to the previous question and showed the sources of opposition preventing the technology from making it into driver's licenses and the role

they played. These same groups could voice similar concern and opposition in future large-scale fingerprint biometric technology implementations.

*Question 5: What factors prevented the legislation from being passed by the senate?*

This question, though similar to the previous question, helped highlight the specific issues raised by opposition or legislators which played a role in preventing the legislation from being passed. These issues are fundamental to most identity management technologies and are important to understand.

*Question 6: Did you feel that Smart-Cards contain sensitive information that could be stolen or shared with others? Did your constituents feel the same way?*

The information held on the IC Chip in the driver's license was the central focus of the debate. This question was asked to determine the degree of sensitivity about the information contained on smart-cards, the perceived security of the technology, and whether or not the representative's constituents agreed with their perceptions.

*Question 7: Did you feel identity theft was a major issue? Did your constituents feel the same way?*

This question was asked to determine the level to which the concern of identity theft played a role in the legislation decision and defeat. It also sought to determine if the legislator's constituents felt the same way in the matter.

*Question 8: Did you feel that privacy invasion was a major issue? Did your constituents feel the same way?*

This question determined the level to which privacy invasion played a role in the legislation decision and defeat of the technology in Utah. It also sought to determine if the legislator's constituents felt the same way in the matter.

### 3.5.2 State of Utah CIO

In addition to state representatives, the current Deputy Chief Information Officer for the State of Utah, Al Sherwood, was contacted in relation to the 1997 legislation. Though not directly involved in the legislation, he was willing to share his knowledge and experience with the technology. A number of questions were asked concerning his perspective on the legislation, the limiting factors of the legislation, the extent to which legislators were educated on the technology, and if he felt situations are any different 8 years later.

## CHAPTER 4 – RESEARCH RESULTS

### 4.1 Phase I Results

The process of extracting a fingerprint from a scanned image was finalized and automated using a combination of the NIST's software and AuthenTec's freeware image capture program. As stated in the previous chapter, the significance of this phase was to (1) educate Phase II respondents on how data is extracted from a fingerprint image in real-time to demonstrate that fingerprint features as opposed to the actual fingerprint are used in biometric systems, and (2) to increase the understanding of the individual researcher of the technology.

#### 4.1.1 Fingerprint Extraction Process

The feature extraction process outlined in Chapter 3 was automated by using a series of simple batch scripts to execute the necessary code. The process worked by running ATImageCapture, a freeware program to capture the image from the scanner. After capturing and saving the image, transform.bat was run. This first script performs operations to transform the image to the correct file type and places it into the correct directory to be operated upon, shown in Figure 4.1. After performing the necessary transactions, it calls extract.sh. Extract.sh, shown in Figure 4.2, is a simple bash script which runs in Cygwin and converts the image file to the formatted AN2K file using the

NIST's software packages, then performs the minutiae extraction and displays the results onto the screen.

```
rename TestUser7v001.bmp image.bmp
cd bmp2raw
bmp2raw c:\image
cd\
rename image.R08 image.raw
move image.raw c:\cygwin\usr\local\nfis\bin
del image.bmp
C:
chdir C:\cvwin\bin
```

**Figure 4.1:** Transform.bat – script for transforming bitmap image to usable raw format

```
cd usr/local/nfis/bin
./txt2an2k nist3.fmt finger.an2k
./mindtct finger.an2k finger.an2k
cat /usr/local/nfis/bin/min.txt
exit
```

**Figure 4.2:** Extract.sh – script for calling txt2an2k and mindtct for viewing fingerprint image data

Figure 4.3 below shows the formatted text file used as the input for txt2an2k to create the AN2K file for minutiae extraction. The formatted text file was named nist3.fmt.

```

1.1.1.1 [1.001]=165_
1.2.1.1 [1.002]=0300_
1.3.1.1 [1.003]=1_
1.3.1.2 [1.003]=1_
1.3.2.1 [1.003]=14_
1.3.2.2 [1.003]=01_
1.4.1.1 [1.004]=NISTDATA_
1.5.1.1 [1.005]=20050101_
1.6.1.1 [1.006]=1_
1.7.1.1 [1.007]=DAI000000_
1.8.1.1 [1.008]=MDNISTVIP_
1.9.1.1 [1.009]=g00418m.an2_
1.10.1.1 [1.011]=19.69_
1.11.1.1 [1.012]=19.69_
2.1.1.1 [14.001]=614557_
2.2.1.1 [14.002]=01_
2.3.1.1 [14.003]=3_
2.4.1.1 [14.004]=MDNISTVIP_
2.5.1.1 [14.005]=20050101_
2.6.1.1 [14.006]=192_
2.7.1.1 [14.007]=192_
2.8.1.1 [14.008]=1_
2.9.1.1 [14.009]=96_
2.10.1.1 [14.010]=96_
2.11.1.1 [14.011]=NONE_
2.12.1.1 [14.012]=8_

```

**Figure 4.3:** Nist3.fmt – formatted text file inputted into TXT2AN2K for minutiae extraction

Nist3.fmt in conjunction with the batch scripts shown above allowed for MINDTCT to extract fingerprint features from the captured image data. After the data was captured, the data was printed to the screen, showing the various parameters of the fingerprint captured. Figure 4.4 below shows the resulting extracted data.

```

0 : 20, 100 : 1 : 0.21 :BIF : DIS : 2 : 48, 43; 1 : 63, 88; 3 : 47, 109; 2 : 27, 154; 1 : 22, 153; 1
1 : 22, 153 : 17 : 0.18 :BIF : APP : 3 : 47, 109; 1 : 63, 88; 3 : 104, 121; 8 : 126, 163; 9 : 27, 154; 0
2 : 27, 154 : 16 : 0.45 :BIF : APP : 3 : 48, 43; 0 : 47, 109; 1 : 63, 88; 3 : 104, 121; 8 : 126, 163; 9
3 : 41, 34 : 18 : 0.83 :BIF : APP : 3 : 136, 16; 8 : 106, 41; 6 : 48, 43; 0 : 63, 88; 3 : 47, 109; 2
4 : 47, 109 : 17 : 0.93 :RIG : APP : 0 : 48, 43; 1 : 63, 88; 1 : 106, 41; 6 : 135, 106; 9 : 104, 121; 6
5 : 48, 43 : 18 : 0.86 :RIG : APP : 0 : 136, 16; 8 : 106, 41; 6 : 46, 75; 11 : 104, 121; 6 : 63, 88; 2
6 : 63, 88 : 17 : 0.73 :RIG : APP : 0 : 106, 41; 4 : 146, 75; 9 : 35, 106; 7 : 104, 121; 4 : 126, 163; 5
7 : 104, 121 : 15 : 0.85 :RIG : APP : 0 : 106, 41; 1 : 170, 40; 8 : 146, 75; 5 : 135, 106; 3 : 126, 163; 0
8 : 106, 41 : 18 : 0.78 :BIF : APP : 3 : 136, 16; 2 : 170, 40; 7 : 46, 75; 4 : 135, 106; 2 : 126, 163; 1
9 : 126, 163 : 30 : 0.94 :RIG : DIS : 1 : 136, 16; 5 : 135, 106; 2 : 146, 75; 5 : 170, 40; 9
10 : 135, 106 : 15 : 0.81 :RIG : APP : 0 : 136, 16; 2 : 146, 75; 2 : 70, 40; 6
11 : 136, 16 : 18 : 0.20 :BIF : APP : 3 : 170, 40; 3 : 146, 75; 1
12 : 146, 75 : 15 : 0.35 :BIF : APP : 3 : 170, 40; 3
13 : 170, 40 : 13 : 0.19 :BIF : APP : 3

```

**Figure 4.4:** Data from minutiae-extraction process

Figure 4.4 shows 13 minutiae detected within an inputted fingerprint image. The individual minutiae were listed from 0 to 12 formatted according to the manual entry for MINDTCT, shown below in Figure 4.5. The data extracted consists of the following: (1) an integer identifier of the detected minutia, (2) x and y pixel coordinate of the detected minutia, (3) the direction of the detected minutia ranging from 0 to 31 in increments of 11.25 degrees, (4) a reliability measure of the detected minutia ranging from 0.0 to 1.0, (5) the type of minutia, either a bifurcation (BIF) or ridge ending (RIG), (6) the type of feature detected, either appearing or disappearing, (7) an integer identifier of the type of feature detected, (8) the x and y coordinates of the first neighboring minutiae, and (9) the ridge count between the detected minutiae and the neighboring minutiae.

```

MN : MX, MY : DIR : REL : TYP : FTYP : FN : NXI, NYI : RCI : ...
where:
MN      is the integer identifier of the detected minutia.
MX      is the x-pixel coordinate of the detected minutia.
MY      is the y-pixel coordinate of the detected minutia.
DIR     is the direction of the detected minutia. Minutia direction is represented similar to ridge
flow direction, only minutia direction is uni-directional starting at vertical pointing up
with unit 0 and increasing clockwise in increments of 11.25 degrees completing a full circle.
Using this scheme, the angle of a detected minutia is quantized into the range 0 to 31
with 8 representing horizontal to the right, 16 representing vertical pointing down, and 24
representing horizontal to the left.
REL     is the reliability measure assigned to the detected minutia. This measure is computed by
looking up the quality level associated with the position of the minutia from the Quality
Map. The quality level is then heuristically combined with simple neighborhood pixel
statistics surrounding the minutia point. The results is a floating point value in the range
0.0 to 1.0, with 0.0 representing lowest minutia quality and 1.0 representing highest
minutia quality.
TYP     is the type of the detected minutia.
bifurcation = "BIF"
ridge ending = "RIG"
FTYP    is the type of feature detected.
appearing = "APP"
disappearing = "DIS"
(This attribute is primarily useful for purposes internal to the minutia detection algo-
rithm.)
FN      is the integer identifier of the type of feature detected. (This attribute is primarily useful
for purposes internal to the minutia detection algorithm.)
NXI     is the x-pixel coordinate of the first neighboring minutia.
NYI     is the y-pixel coordinate of the first neighboring minutia.
RCI     is the ridge count calculated between the detected minutia and its first neighbor.
for each additional neighbor ridge count computed, the pixel coordinate of the neighbor
and the ridge count to that neighbor are reported.
...

```

**Figure 4.5:** MINDTCT minutiae data format

#### 4.1.2 Conclusions of Phase I

This process and the resulting data demonstrate how features can be extracted from fingerprint images. A working biometric system would use a hash or encryption key to encrypt various parameters similar to those previously described in this process. The data served the purpose of demonstrating the operation of fingerprint biometric systems and their use of electronic data representing features of a fingerprint rather than the actual fingerprint image.

This research was performed to facilitate an understanding of how biometric fingerprint data extraction and template creation occurs in fingerprint biometric systems. Additionally, this research was necessary to better understand the process by which most fingerprint biometric systems capture fingerprint data and to use as a tool to educate Phase II respondents on how fingerprint parameter data, but not the actual fingerprint itself, are used. This process allowed for some respondents involved in Phase II to see how the fingerprint extraction process works and help them to understand that fingerprint data were extracted for identification – entire images were not used.

## 4.2 Phase II

### 4.2.1 Demographic Data

Approximately 170 surveys were gathered in this phase of research. The raw data and graphs analyzing the data can be found in Appendix A in this chapter. Analysis of the demographic data show that of all of the respondents, more than half were male and the majority of respondents were between the ages of 18 and 25 with very few respondents over the age of 60. The respondents were asked to rate their overall level of technical expertise related to technology, and responses were evenly divided between



high, medium, and low technical expertise with the majority of responses being 'low'. When asked about the highest level of education attained, nearly 75% responded to having at least completed some college course work, and about half possessed at least a bachelors degree or higher. Only about 15% possessed an advanced degree. More than one-third of all those surveyed had the technology and the fingerprint extraction process of Phase I demonstrated to them. This demographic data was primarily used to validate that the surveyed population was representative of various demographic groups. Additional analysis of the results has been performed which includes some demographic information.

The results of this survey were considered representative of the majority of education, technology, and government employees around the Salt Lake and Utah County areas in Utah since more than a sufficient sample size was used and random individuals were chosen from each location. Inference to other populations in the State of Utah and beyond regarding these results should not be made since the population is not representative of the entire state or beyond.

#### 4.2.2 Question 1

The first question asked if any of the respondents had ever been victims of identity theft. Nearly 90% of all respondents had not been victims of identity theft in any way. After analyzing the proceeding questions based upon the results of this question, those who had been victimized before did not have statistically different responses to the other questions as compared to those who had not been victimized, nor did they have more concerns with the technology than those who had not been victimized. This

indicates that previous identity theft, in this case, had little effect upon the perceptions of fingerprint biometric technology.

#### 4.2.3 Questions 2-4

The second question quantified the level to which security was more important than convenience in general among the surveyed population. Eighty percent of those surveyed answered with a response of 5 or greater, meaning they believe security was more important than convenience. Analysis of these responses showed that the responses to this question were not greatly correlated to the responses to the remaining questions. Of the respondents of this survey on a scale of 7 with 7 denoting high, slightly more individuals from technology background answered between a 5 and 7 than those from other backgrounds. Regarding question three and four, nearly 90% expressed unfamiliarity with the technology answering with a 3 or lower, and about the same percentage responded as having never used a fingerprint scanner before. Those who had used a fingerprint scanner before did not appear to understand the technology any better and did not have differing responses to the proceeding questions.

#### 4.2.4 Question 5

Each individual surveyed was asked about concerns she would have about using her fingerprint for identification purposes. The majority of those surveyed responded with no initial concerns with using their fingerprint for identification. Of those concerns voiced, the majority responded with the concern of data accessibility by individuals other than those administering the biometric system. Second to this concern was the threat of identity theft as a result of using one's fingerprint and privacy issues. The remaining

concerns consisted mostly of general security issues, system reliability, and system accuracy. The graph shown in Appendix A for question 5 shows all of the different concerns voiced and the percentage of respondents who voiced each concern. The results of this question would suggest that the majority of individuals do not have negative perceptions of the technology. However, the results of the final question of the survey indicate otherwise.

#### 4.2.5 Question 6

The next question relates to the perceived level of privacy invasion among the surveyed population. More than half of all respondents answered a 3 or lower, corresponding to fingerprint scanning not being considered an invasion of privacy. This answer was mostly consistent among age, sex, and education. Most respondents between the ages of 18-25 answered with a 3 or lower, while the responses of those over 25 were more varied. Respondents working in a technical field responded with a 3 or lower more often than those working in an education or government occupation. The vast majority of education workers surveyed answered a 4 or lower and government workers were more evenly distributed along the spectrum of answers. The lower level perceived privacy invasion among higher technically-oriented respondents could be attributed to the tendency of technically-oriented individuals to accept new technologies more readily than non-technical individuals.

Overall, it appears that privacy invasion was not a serious issue among the population, but may be a greater issue specifically for non-technical individuals and those over the age of 25. Users may have greater concerns over privacy invasion depending on the data being protected by their fingerprints. Based on the results of this question, a

system targeted at a non-technical organization should be sure to educate users as to issues of perceived privacy invasion.

#### 4.2.6 Question 7

Question 7 sought to determine the perception among the population concerning the ease of copying or stealing a fingerprint in general. Roughly 50 % of the surveyed population responded with a 3 or lower corresponding to a belief that stealing or copying fingerprints is difficult. The majority of these individuals were between the ages of 36 to 60. Respondents younger than 36 had more varied responses to the question. Education and occupation did not appear to have an effect upon the results.

The results of this question suggest that there is not a clear understanding among this population of whether or not fingerprints are easily stolen or copied. Therefore, education meant to inform users of the realities of biometric technology should include information specific to the system implemented and seek to reassure users that a stolen or copied fingerprint would unlikely pass as a legitimate fingerprint. Addressing this concern was important since users believing their fingerprint could be copied and used to impersonate them would have trepidation about using such a system.

#### 4.2.7 Question 8

The next question was more specific regarding stolen or copied fingerprints by specifying fingerprint scanners in public settings. The responses were distributed evenly between 3 and 5, corresponding to an average response between 'difficult' and 'easy'. This suggests that the population was unsure as to the possibility of stealing or copying a fingerprint from a public fingerprint scanner just as they were unsure about stealing or

copying of a fingerprint in general. The only major response variation was the slight difference between those individuals who had received the technical demonstration and those who did not. Sixty-five percent of those who did receive the demonstration answered with an average response of 4 or lower to the question whereas 53% of those who did not receive the demo answered this way. This suggests that demonstrating fingerprint scanning technology influences individuals to believe fingerprint copying or theft is difficult in public settings. Therefore, an organization implementing a fingerprint biometric system would be wise to demonstrate or offer a high-level explanation of how a fingerprint scanning system operates in order to facilitate user acceptability.

#### 4.2.8 Question 9

Question 9 on the survey dealt with the concern of data accessibility by third parties. The majority of the surveyed population replied to the question with a response of 5 or greater, corresponding to a response of ‘very concerned’. Respondents with a low level of technical expertise tended to respond with higher levels of concern than those with medium or high technical expertise. Though only comprising roughly 15% of the total surveyed population, more than half of all respondents over the age of 46 answered with a 6 or 7 to the question. Thirty-eight percent of those in a technology occupation answered with a response of 5 or more compared to 51% of education and 65% of State of Utah employees. Based on the results of this question, organizations where the working population was older and not technically oriented can expect the concern of outside access of fingerprint data voiced. Similarly, non-technical industries could expect concern over this issue more than other industries. It is unlikely for an organization to share fingerprint information with other parties. Even if the information

were accessed illegally by an outside entity, its usefulness would be non-existent without extensive knowledge of the extraction and encryption algorithm. Nevertheless, the concern and in-place security should be addressed by an organization's training and tutorial for their fingerprint system to alleviate this concern.

#### 4.2.9 Question 10

The next question pertained to the legality of obtaining and using employee fingerprints by employers. The responses to this question were evenly distributed among the seven choices. Interestingly, nearly half of the respondents over the age of 36 responded with an answer of 6 or 7, corresponding to a response that organizations possess the right to have their employee's fingerprints on record. Only about 17% of those under the age of 36 responded similarly. Among those occupations targeted by the survey, government employees felt that organizations hold the right to fingerprint their employees more than technology and education employees. The majority of respondents who had the technology demonstrated to them answered similarly. The issue of legality does not appear to be a major concern based upon the results. However, an organization should clearly state their policy of fingerprint gathering and usage in order to avoid potential law suits by employees. Legal issues should be addressed, but past legislation which has predominantly ruled in favor of entities gathering fingerprints.

#### 4.2.10 Question 11

Question 11 asked about reconstructing a fingerprint image from electronic biometric data. Most responses to this question were in the middle of the spectrum, between 3 and 5, correlating to a response somewhere between 'not possible' and 'easily

reconstructed'. This suggests that the possibility of reconstructing fingerprint images from raw data was not clear among the population. In terms of the various demographics, more government and education employees answered between 1 and 3 than technology workers. Also, more respondents who had the technical demonstration shown to them answered between a 5 and 7 than those who had not.

The reality of reconstructing fingerprint images from raw data is that it is nearly impossible. Because the data gathered from fingerprints is only a small percentage of the whole fingerprint and algorithms used to create unique templates vary between systems, reconstruction of a fingerprint image is highly improbable. The results of this survey suggest technically oriented individuals and those who have seen the technology in operation would have the greatest concern with fingerprint data reconstruction. In a technology-based organization, the improbability of reconstructing fingerprint images from data should be addressed along with demonstration of the system.

#### 4.2.11 Question 12

The next question sought to measure the level of religious or moral objection to fingerprint biometric technology. Nearly 80% of all respondents answered a 1 or 2, indicating the majority of respondents would have no moral or religious objections to using their fingerprint for identification purposes. The only responses of 5 and over came from those who rated themselves as having low technical expertise. It is important to note that while only low-technical expertise individuals had significant moral or religious objections to using fingerprints for identification purposes, this population only comprised 15% of the surveyed population with low technical expertise. It can be inferred that little concern would be voiced about the morality of using one's fingerprint,

particularly in a high-tech industry. Nevertheless, these results show that the objecting minority exists, particularly among populations of low technical expertise. These are issues which would likely be tied to a person's beliefs and values, making it nearly impossible to educate a population opposed to the technology based on moral or religious reasons. As seen with the Smart Card Driver's Licenses in Utah and explained in Section 4.4, the minority groups who were against the technology were the main reason it never came to fruition. Therefore, it is highly likely that even a small population in opposition to fingerprint biometric technology could cause enough opposition to prevent the technology's acceptance.

#### 4.2.12 Question 13

Question 13 sought to determine the level to which health concerns such as germs, electrical shock, or pain were associated with fingerprint scanning among those surveyed. The vast majority of those surveyed did not have any health concerns. About 90% of all respondents answered with a 3 or less, corresponding to no perceived health hazard. Those respondents working in a technological field, with high-technical expertise, and who had the technical demo were more likely to respond with a 1. Very few answered with anything greater than a 2. For the statistically few individuals believing a health hazard exists with fingerprint biometrics, education clarifying that the technology is no more hazardous than pushing an elevator button or opening a door should be emphasized. However, this concern does not appear to be prevalent among the population and probably need not be addressed.



#### 4.2.13 Question 14

The next question determined the perceived accuracy of fingerprint scanning technology among the population. Seventy-two percent of the population responded with a 5 or higher, corresponding to the perception that fingerprint scanners are very accurate. No dramatic statistical variation between responses existed among the demographics of age, sex, or occupation. About 75% of those who described themselves as having a high technical expertise answered with a 5 or higher, a higher percentage than those with a lower technical expertise. These results suggest that accuracy should clearly be stated to the user population of a proposed biometric system to reassure individuals with low technical expertise.

An unexpected result of this survey was the larger percentage of respondents who did not have a technical demo and yet answered with a 5 or higher. Though the demonstration almost always accurately identified individuals on the first attempt, the respondents receiving the demonstration appeared to often question the technology's accuracy. Any one of the following reasons could explain this anomaly:

1) Viewing the technology in action very briefly suggested to some the possibility that it would not work perfectly each time. Perhaps the population did not think they were being shown everything.

2) A limited number of fingerprint scans were performed in each demonstration. Perhaps more scans would suggest a higher system accuracy.

3) The occasional false reject occurring in the demonstration suggested the inaccuracy of the system.

#### 4.2.14 Question 15

Question 15 asks about how comfortable the sample population would be using a fingerprint to enter their place of employment. Nearly 65% of the population responded with a 5 or higher, indicating they would be comfortable using their fingerprint for identification in order to gain entry to their place of employment. Of those who received the demonstration, 71% responded with a 5 or higher. The majority of both technology and government workers responded similarly. Those working in an educational field answered with lower numbers, however. A likely explanation for this result is the number of technology and government workers who already use an electronic form of personal identification for building access. Novell uses electronic name badges, and various government offices including Utah State Parks and Recreation require a special token or badge for access. Consequently, those who commonly use badges or other electronic access methods may be more willing to use a fingerprint for building access than those who do not. It can be assumed that a biometric system would gain greater user acceptance among technology, government, and other offices for building entry where an existing identity management technology already exists. Hence, it could be assumed that adequate instruction should be given to those using a system in an educational environment. Additionally, demonstration of the technology would likely aid user acceptance of the technology for building access among populations not previously introduced to technological approaches for identity purposes.

#### 4.2.15 Question 16

The next question determined if the population views fingerprint biometrics as more convenient than other common security measures. Nearly 3 out of 4 respondents

answered with a response of 5 or higher which corresponds to a belief that fingerprints are more convenient than other security measures. Among the various demographics, no major statistical differences among education, technical expertise, or other demographics had an effect upon the response. This suggests that the convenience of fingerprint biometric technology is quite well established among the surveyed population and does not need to be greatly reinforced to a potential biometric system user base.

#### 4.2.16 Question 17

Question 17 addresses the question of fingerprint biometric security as compared to other common security measures. Seventy-five percent of all respondents gave a response of 5 or greater, corresponding to fingerprint biometrics as more secure than other common security measures. Nearly 85% of all respondents over the age of 46 responded with a 5 or higher, suggesting that those over the age of 46 believe fingerprint biometric technology is more secure than other methods of security. In terms of occupation, individuals working in an educational setting answer lower compared to those working in technology and government departments. Again, this could be attributed to the fact that those working for Utah State Parks and Recreation and Novell use and are familiar with security tokens like swipe cards and magnetic media for building access. Therefore, a lesser-known and perceivably emerging technology such as fingerprint biometrics may be seen as new, different, and superior in terms of security. Regardless of the population, an organization implementing a fingerprint biometric system should educate the user base to the security of the technology in order to facilitate user acceptance. This is critical in today's society where security is of paramount

importance. A population with security concerns regarding an identity management system would obviously be hesitant about enrolling in it.

#### 4.2.17 Question 18

The final question of the survey addressed any concerns held by the population after having participated in the survey. It sums up the survey by highlighting those concerns which were paramount among the surveyed population. Because the majority of people were unfamiliar with fingerprint biometric technology, this question was posed after the previous specific questions in order to better determine the perceptions among the population. Interestingly, of the 170 individuals participating in the survey, the number of individuals without concerns dropped from 93 to 23 since question 5 was asked and this question 18. This was not surprising since (a) respondents were generally unfamiliar with the technology and would not know what to be concerned about, and (b) because specific areas of concern were asked about in the survey. The majority of concerns voiced in question 5 were also expressed in question 18. However, the numbers of respondents voicing the same concerns in question 18 were higher in each case. The concerns which had the most number of respondents include overall system security, privacy, third party data accessibility, data protection, and system accuracy. These results show that concerns exist regarding fingerprint biometric technology. The negative perceptions of the technology held by the population in this research would likely comprise a large percentage of concerns likely held by users of a newly implemented fingerprint biometric system in technology, education, or government settings in the State of Utah.

#### 4.2.18 Conclusions of Phase II

There were a number of significant conclusions which could be drawn from these results. The voiced concerns from the surveyed population give an excellent guideline as to details which should be addressed during a user education or training session. Though few concerns were voiced initially by question 5 in the survey, the results of the final question 18 in the survey indicate that there were concerns among the sample population. This difference in level of concern has a few possible explanations:

1) An increased understanding of the technology resulting from the survey questions may have lead to a more thoughtful response to question 18.

2) The wording of question 18 had slightly different wording than question 5. Respondents may have felt a response was warranted for question 18 more so than question 5.

3) In many cases, respondents appeared not to have previously given thought to the questions raised in the survey which likely prompted a more thoughtful response to the final survey question.

The results of the privacy invasion question had mixed responses, yet the results of the final question rated privacy issues as the second most voiced concern central to the technology. Privacy is an issue which affects people differently. Some people are strongly opposed to any form of identification stored electronically while others are indifferent. Therefore, privacy is an issue which may not easily be overcome through education. Fingerprint copying and theft did not arise as a major concern among the population. However, individuals were unsure about fingerprint fraud in a public fingerprint scanning system compared to fingerprint fraud in general. Therefore, it should be clarified that it would not be any easier to commit fingerprint fraud on a public

fingerprint scanner than it would be on an individual's personal fingerprint scanner, and that current fingerprint scanning technology continues to improve by including various "liveness" checks.

Third party data accessibility was a concern among the surveyed population. The majority of the surveyed population voiced concern over the possibility over outside access to fingerprint information in question 9, and approximately 11% specifically noted it as the most significant issue with the technology. It should be clarified in user training that most fingerprint biometric systems differ in the algorithm used to encrypt and store fingerprint information, making third party data accessibility highly improbable. Tied to this concern is the possibility of fingerprint images being reconstructed from captured biometric fingerprint data. This concern can be alleviated by noting the small percentage of fingerprint information extracted from fingerprints, making reconstruction of a complete fingerprint from the captured data nearly impossible.

Legislation dictating whether or not an employer can legally require employees to enroll in a biometric system is not firmly established. Past court proceedings relating to fingerprint capture and usage have ruled in favor of the entity requesting the fingerprint information. Many of the survey respondents, especially those 36 and over, felt that organizations hold the right to require fingerprint information from employees. It would be wise for an organization to specify their right to obtain fingerprint information from employees as standard employee screening for all applicants in their human resource policy to avoid any potential lawsuits. Past court cases indicate resolution in favor of the employer or biometric administrator. Two court cases mentioned in the literature review, *Christopher Ann Perkey v. Department of Motor Vehicles* and *Utility Workers Union of*

*America v. Nuclear Regulatory Commission*, both ruled in favor of the entity requiring the fingerprint sample.

Issues of morality and health were the two concerns that registered the lowest number of favorable responses. There will always be a small percentage of individuals who exhibit such concerns. Health concerns can be addressed by comparing using a fingerprint scanner to pushing an elevator button or pressing a button on a drinking fountain. Moral or religious objections are more difficult to overcome since these concerns are tied to core moral values. An awareness that politically extreme right or left employees may object to using their fingerprint should exist in the organization. It may take a number of years and a proven track record of fingerprint biometric system usage before moral objections to the technology disappear.

Although the accuracy of fingerprint scanners varies from by vendor, the majority of currently available scanners are very accurate. This perception of accuracy was held by the majority of those with a high technical expertise. For an organization where the technical expertise of its employees is not high, the accuracy of the system needs to be highlighted and ideally demonstrated during user training. Users who are concerned that the system could misidentify one person for another would be unlikely to accept a biometric security system.

The survey results suggest the majority of users believe that fingerprint biometrics are secure and convenient, particularly where users already use identity management technology. In industries where existing security technology has not been used, the convenience and security of fingerprint biometrics should be stressed. Overall, the responses to the survey proved a valuable baseline of those concerns present among the target population. Certain demographics appeared to be more important than others.

Education level, age, and sex did not appear to have the same impact as technical expertise, occupation, and whether or not the demonstration was received. These concerns serve as the basis for those questions asked in Phase III of this research. Phase III shows the extent to which education changed the level of concern among the surveyed population and leads to concluding the degree to which education affects user opinions on fingerprint biometric technology.

### 4.3 Phase III

#### 4.3.1. Demographic Information

Each of the 170 respondents who gave a contact email address was asked to participate in this phase, Phase III, of the research. Of the 170 respondents in Phase II, a total of 142 respondents (84% of original survey) participated in this present phase of the research. To facilitate the process of sharing the fingerprint technology overview, the overview and survey were presented in an online format. Because of anticipated trepidation of requiring personal information such as name, age, and occupation, this information was optional. Therefore, this survey does not take into account these factors to the extent they were in Phase II of the research. Only individuals who had participated in the initial survey participated in the online survey. The main focus of this survey was to compare the overall responses of the initial survey to the responses to the online survey to quantify the level of change resulting from the biometric education. This was an acceptable focus since the education was geared toward a general audience rather than a specific, targeted demographic. Of the questions asked in the first survey, 11 of the same questions were asked along with additional questions that addressed the perceived



effectiveness of the education. The remaining 7 questions were not asked for the following reasons:

1) Question 5 and 18 were not asked since they were used in the first survey to establish the population's initial concerns regarding the technology.

2) The first four questions of the Phase II survey were asked to establish the population's experience and background with issues relating to fingerprint biometric technology.

3) Question 12 which asks about religious and moral objections was not asked since these concerns were not addressed by the education.

All data and graphs of the results are found in Appendix B.

#### 4.3.2 Questions from the Original Survey

##### 4.3.2.1 Question 1

The first question corresponds to question 6 of the original survey which asked about the perceived level of privacy invasion stemming from biometric fingerprint technology. Of all respondents, nearly 70% answered with a 1 or 2, corresponding to fingerprint scanning as not an invasion of personal privacy. This was an increase of 23% as compared to the approximately 47% who responded with a 1 or 2 in the original survey before taking the online survey. Additionally, 32% originally responded with a 4 or greater, corresponding to fingerprint technology being an invasion of privacy, while only 14% in the second survey responded likewise. These results suggest that the online statements on fingerprint biometric privacy affected respondents' perceptions, leading them to believe that privacy is not invaded as a result of using the technology. The

increase in favorable response to this question is significant. Users believing that privacy is not invaded would likely accept a biometric system more so than those who believe that privacy is invaded.

#### 4.3.2.2 Question 2

The next question in the survey corresponds to question 7 on the original survey which asked about the perceived difficulty of copying or stealing a fingerprint. Among those surveyed, 77% responded with a 3 or less corresponding to the belief that it is difficult to steal or copy a fingerprint. In the original survey, only about 55% responded with a 3 or less to the same question. This was approximately a 22% increase in the favorable response of a 3 or less to this question. Though this concern was not specifically addressed in the technology overview, security and safety were stressed. The difficulty of spoofing a fingerprint scanner was addressed, likely precipitating the perception of the difficulty of copying or stealing a fingerprint. In reality, a fingerprint can be copied or stolen from a latent print, but cannot easily be used to fool a fingerprint scanner. The results of this question show that though not directly addressed, education stressing the security of fingerprint biometric technology can sway perceptions significantly.

#### 4.3.2.3 Question 3

Question 3 corresponds to question 8 of the original survey regarding stealing or copying a fingerprint from a publicly-used fingerprint scanner. About 56% of respondents answered with a 3 or lower, analogous to a belief that it is difficult to steal or copy a fingerprint from a public fingerprint scanner while about 40% responded similarly

in the first survey. This increase of 16% more favorable responses was significant, particularly since this issue was not explicitly addressed on the education page. This increase was likely due to the stressing of safety and security, resulting in the increased perception of safety from the copying or theft of fingerprints from a public scanner.

#### 4.3.2.4 Question 4

The next question was the same as question 9 of the previous survey which asks about data being distributed, access, or shared by third parties. In the original survey, respondents answered with a 3 or lower 32% of the time compared to 65% of respondents in this survey. The 33% increase was likely due to privacy being directly addressed in the education. It appears the statements on privacy had enough of an effect on survey respondents to significantly reduce the level of concern of third party data access. These results suggest a significant impact on respondents due to education. In real-life settings, user education and training should be specific about entities granted access to the data. In most cases, the data is only used within the organization for identification through the company's specific biometric system. Stating this fact in conjunction with those privacy issues highlighted in this education could significantly reduce the level of this concern.

#### 4.3.2.5 Question 5

Question 5 of the online survey mirrors question 10 of the original survey pertaining to the legality of fingerprint retrieval and usage by employers. Approximately 42% of all respondents answered with a 5 or higher originally, corresponding to employers possessing the right to legally require a fingerprint to be given. The second survey measured 62% of respondents answering with the same response. The legality of

fingerprint usage by employers was directly addressed by the user education, and notes that past court cases tend to favor the employer in legal battles over fingerprinting. This information was likely the cause of the increase in favorable responses on the legal issues of fingerprint usage. Organizations implementing biometric fingerprint systems must obtain the fingerprint non-intrusively and use it only for legitimate purposes in order to be within legal limits. Employers should initiate human resource policy concerning fingerprint usage to avoid any potential legal problems.

#### 4.3.2.6 Question 6

The next question addresses reconstructing fingerprints from raw biometric data, the same question as question 11 from the first survey. Originally, about 37% of respondents answered with a 3 or lower corresponding to reconstruction of data as difficult and 67% answered similarly in the second survey. The increase in respondents believing it is difficult or impossible to reconstruct a fingerprint from raw data likely stems from the statements stressing this point in the education. It was important to stress the improbability of reconstructing fingerprints from raw data to alleviate this concern. The results of this question suggest the brief statement written in this education effectively swayed perceptions toward the reality of this security facet.

#### 4.3.2.7 Question 8

Question 8 of the online survey asks about perceived health risks resulting from using a public fingerprint scanner. Few respondents believed any health risk was posed initially, and similar results came from this survey. The numbers of respondents answering with a 1 or 2 changed from 85% to about 92% between the two surveys.

These results suggest that health risks are not a source of major concern among the general population. A slightly larger percentage of individuals responded with a 1 or 2 to the question resulting from the direct addressing of the lack of potential health risks associated with fingerprint scanners. Though this perception was minimal, the issue of health should still be addressed by employers when educating users on a fingerprint biometric system.

#### 4.3.2.8 Question 9

This question pertains to the perceived accuracy of fingerprint biometric scanners, mirroring question 14 of the original survey. The difference in numbers answering the question favorably varied from 75% of respondents answering with a 5 or greater compared to roughly 89% of similar responses. The statement stressing the system's accuracy probably caused the slight increase in this perception. Though the statement did not site a specific source, the majority of respondents believed in the accuracy of the technology.

#### 4.3.2.9 Question 10

The next question on the survey corresponds to question 15 on the original survey, asking how comfortable the respondent would be with using their fingerprint to enter a building. 88% of the respondents of this survey answered with a 5 or higher, corresponding to individuals being comfortable using their fingerprint to enter the building they work in, contrasted with the 64% of individuals answering similarly in the original survey. These results suggest the facts concerning the technology reassured

individuals regarding building access and it can be concluded that education has helped increased user acceptance of the technology in terms of building access.

#### 4.3.2.10 Questions 11-12

The next two questions, mirroring questions 16 and 17 on the original survey, ask about the perception of superior convenience and security of fingerprint biometrics as compared to other common security measures in general. In terms of convenience, about 93% of individuals responded with a 5 or higher, corresponding to a belief that fingerprint biometrics are more convenient than other measures, and 73% responded with a 5 or higher in the original survey. This increase of 20% answering favorably could be traced to the stressing of convenience by the education page shared with respondents. The perceived level of security compared to other security measures was also asked in both surveys, with a response of 5 or higher to this question, corresponding to a perception of fingerprint biometrics being more secure than other security measures, made by 75% of respondents in the original survey and 85% of respondents in this survey. This increase was not as significant as the increase in responses to the convenience question and may be tied to the education.

#### 4.3.3 Additional Survey Questions

##### 4.3.3.1 Question 7

Aside from those questions which had been asked in the original survey, other questions were asked to measure the effectiveness of the survey. The degree to which the education reassured each respondent about fingerprint biometrics in general was asked.

76% of respondents answered with a 5 or greater, corresponding to an increased general reassurance regarding the technology's validity. This suggests that overall, the education was reassuring to the majority of respondents and they felt more comfortable with the technology as a valid identity management solution. Similar education and training in a live setting would likely reassure to users of a new system as well, according to these results.

#### 4.3.3.2 Questions 13-14

Two questions regarding respondents' willingness to use public fingerprint scanners were asked; one asks how willing they would then be to use the technology in their place of employment, and the other in a commercial location. Of all respondents, 80% answered with a 5 or greater which corresponds to a willingness to use a public fingerprint scanner in their place of employment. Only 52% said they would be more willing to use a public fingerprint scanner in a commercial location than they were previous to the education. Obviously, there was trepidation among the respondents concerning fingerprint usage in a commercial setting compared to usage within their own place of employment since the two figures differ by nearly 30%. Such a fear should be directly addressed by the management of the system. Since commercial systems would likely involve monetary transactions, concern about using one's fingerprint in a commercial setting would cause trepidation. Additional user education and training may need to take place to overcome concerns of fingerprint scanner usage for commercial use.

#### 4.3.3.3 Question 15

The final question of the survey asks about the degree to which the online information page helped the respondents better understand how biometric technology works. Eighty-six percent answered with a 5 or greater, corresponding to an increased understanding of how the technology works. Facilitating users' understanding would logically lead to a higher rate of acceptance of the technology. Respondents appeared to learn more about the technology simply through the brief overview given. Similarly, users of a newly implemented biometric system would likely learn more through a detailed overview of the system.

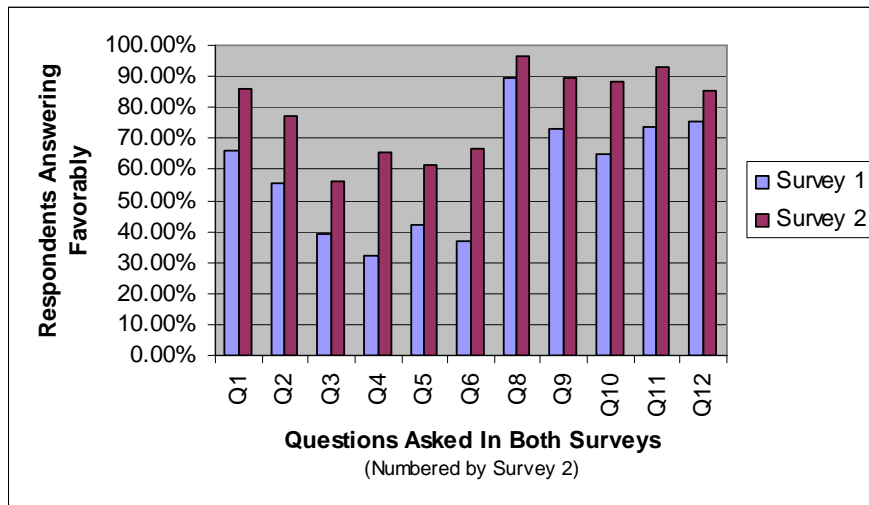
#### 4.3.4 Conclusions of Phase III

To some extent, education played a role in alleviating the concerns of those respondents participating in both surveys. This conclusion can be summed up by tables 4.1, 4.2, and Figure 4.6 below. A 7-point Likert Scale was used for the questions in both surveys, so a response of 1-3 was considered a favorable response to those questions where a response of 1 was considered optimal. Likewise, a response of 5-7 was considered a favorable response to those questions where a 7 was considered optimal. The favorable response in the graph below varies from question to question. As seen in Figure 4.6 and Table 4.1 below, each question had more favorable responses in the Phase III survey compared to the Phase II survey. Table 4.1 shows an algebraic analysis that illustrates the increase of favorable responses ranging between 7.07% and 33.14%. The average increase in responses between questions from Phase II to Phase III was favorable, around 19%. Figure 4.6 gives a graphical representation of the difference between favorable responses between the Phase II survey and the Phase III survey.



**Table 4.1:** Difference in favorable responses from Phase II to Phase III

Question (Numbered According to Phase II Survey)	Phase I Favorable Responses		Phase II Favorable Responses		Difference
	Total	Percentage	Total	Percentage	
	1 To what degree would you consider fingerprint scanning an invasion of your personal privacy?	112	65.88%	122	
2 How easy do you think it is for fingerprints to be stolen or copied?	94	55.29%	110	77.46%	Phase II, +22.17%
3 After using a fingerprint scanner in a public setting, how easy do you think it would be for your fingerprint information to be stolen?	67	39.41%	80	56.34%	Phase II, +16.93%
4 After using a fingerprint scanner in a public setting, how concerned would you be about your fingerprint information being distributed, shared, or accessed by a 3rd party?	55	32.35%	93	65.49%	Phase II, +33.14%
5 Can any organization you work for legally require you to give your fingerprint?	72	42.35%	87	61.27%	Phase II, +18.91%
6 Can a fingerprint be reconstructed from raw biometric (electronic) data?	63	37.06%	95	66.90%	Phase II, +29.84%
8 To what degree would you consider using a fingerprint scanner hazardous to your health (i.e. pain, electrical shock, germs)?	152	89.41%	137	96.48%	Phase II, +7.07%
9 How accurate do you think fingerprint scanners are?	124	72.94%	127	89.44%	Phase II, +16.50%
10 How comfortable would you be with using your fingerprint to enter the building you work in?	110	64.71%	125	88.03%	Phase II, +23.32%
11 To what degree would you consider a fingerprint more convenient than other security measures?	125	73.53%	132	92.96%	Phase II, +19.43%
12 To what degree would you consider using a fingerprint more secure than other security measures?	128	75.29%	121	85.21%	Phase II, +9.92%



**Figure 4.6:** Respondents answering favorably in both surveys

Table 4.2 shows an important statistical analysis of the survey data. Two important calculated data show the statistical difference between Phase II survey responses and Phase III survey responses. The first piece of information is the difference between the standard deviations of responses in Phase II and Phase III. The second important piece of information is the effect size between Phase II and Phase III.

Table 4.2 shows a difference between each standard deviation from Phase II to Phase III, with each standard deviation in Phase III being less than standard deviations in Phase II. A lower standard deviation from the mean suggests lower variations in responses to the survey questions. So in addition to more Phase III responses being favorable responses, there was also less variation between responses in Phase III, suggesting that the education helped shape favorable opinions regarding fingerprint biometric technology.

The second highly important statistic gathered from the data, shown in Table 4.2, is the effect size between Phase II and Phase III. Effect size is a metric which measures the magnitude of a treatment effect, in this case the effect of education on the responses in Phase III of this research. It is calculated by dividing the difference of the control and experiment group means by the pooled standard deviation of the two groups. Minus or plus signs indicate a direction of difference, not magnitude of difference. The direction of differences shown in Table 4.2 is due to the Likert scale used to measure responses. Some questions have favorable responses ranging from 1 to 3, while others have favorable responses ranging from 5 to 7. Therefore, a negative effect size for favorable responses ranging from 1 to 3 and a positive effect size for favorable responses ranging from 5 to 7 are both considered favorable changes. The direction for favorable changes is listed next to the question numbers in Table 4.2. In general, effect sizes from 0 to .35 are

considered small, .36 to .60 considered medium, and .61 or greater are considered large. As seen below in Table 4.2, questions 4 and 11 indicate large effect sizes, and questions 1, 3, 5, 6, 9 and 10 indicate medium effect sizes. These numbers indicate the treatment used in Phase III did have a meaningful effect upon responses.

**Table 4.2:** Standard deviation and effect size analysis table

Question Numbers and Directions of Favorable Change (Numbered by Phase II)	DATA ENTRY						RAW DIFFERENCE					STANDARDISED EFFECT SIZE				
	Phase II Responses (Control group)			Phase III Responses (Treatment Group)			pooled standard deviation	Mean Difference	Standard Deviation Difference	Confidence Interval for Difference		Effect Size	Standard Error of E.S. estimate	Confidence Interval for Effect Size		Effect Size based on control gp SD
	mean	n	SD	mean	n	SD				lower	upper			lower	upper	
Q1, -	2.80	170	1.67	2.23	142	1.37	1.54	-0.56	-0.29	-0.91	-0.22	<b>-0.37</b>	0.11	-0.59	-0.14	<b>-0.34</b>
Q2, -	3.15	168	1.75	2.63	142	1.27	1.55	-0.52	-0.48	-0.86	-0.17	<b>-0.33</b>	0.11	-0.56	-0.11	<b>-0.30</b>
Q3, -	4.13	169	1.72	3.30	142	1.54	1.64	-0.82	-0.17	-1.19	-0.46	<b>-0.50</b>	0.12	-0.73	-0.28	<b>-0.48</b>
Q4, -	4.47	170	1.82	3.15	142	1.63	1.74	-1.32	-0.18	-1.71	-0.94	<b>-0.76</b>	0.12	-0.99	-0.53	<b>-0.73</b>
Q5, +	3.99	168	2.08	4.81	142	1.90	2.00	0.82	-0.18	0.38	1.27	<b>0.41</b>	0.12	0.19	0.64	<b>0.40</b>
Q6, -	3.89	165	1.71	3.01	142	1.68	1.70	-0.88	-0.02	-1.26	-0.50	<b>-0.52</b>	0.12	-0.75	-0.29	<b>-0.52</b>
Q8, -	1.71	169	1.09	1.49	142	0.85	0.99	-0.22	-0.24	-0.44	0.00	<b>-0.22</b>	0.11	-0.44	0.00	<b>-0.20</b>
Q9, +	5.29	168	1.24	5.89	142	1.09	1.17	0.60	-0.15	0.34	0.86	<b>0.51</b>	0.12	0.29	0.74	<b>0.49</b>
Q10, +	4.98	169	1.68	5.83	142	1.24	1.50	0.85	-0.44	0.52	1.19	<b>0.57</b>	0.12	0.34	0.80	<b>0.51</b>
Q11, +	5.27	170	1.64	6.15	142	1.13	1.43	0.88	-0.52	0.56	1.20	<b>0.61</b>	0.12	0.39	0.84	<b>0.54</b>
Q12, +	5.37	170	1.36	5.68	142	1.13	1.26	0.30	-0.22	0.02	0.58	<b>0.24</b>	0.11	0.02	0.46	<b>0.22</b>

This increase in favorable responses was due in large part to the educational technical overview given to the respondents. Incidental bias, such as taking the survey online as opposed to in person, may have played a small role, affecting opinions in either a negative or positive way. Nevertheless, it can be concluded that education does play a role in altering user opinions. The numbers shown in the table and figure below indicate significant increases in favorable responses to the posed questions.

The results of this section of the research suggest the hypothesis stated in Chapter 1 is true – a population who has received education regarding the facts of fingerprint biometric technology does exhibit higher levels of acceptance and understanding of the technology and exhibits lower levels of concern measured as a percentage of the surveyed population as compared to the levels measured previous to education. Clearly, user perceptions are an important consideration of any fingerprint biometric system implementation. As Giesing concluded in his study, mentioned in the literature review, “user perceptions with regard to security and privacy considerations were identified as social factors that need to be addressed as part of user adoption when making use of biometrics as an identification method.”

#### 4.4 Phase IV

##### 4.4.1 Contacted Representatives

Representatives involved in the 1997 Driver’s License Smart Card legislation were contacted with questions concerning the issue. In all, a total of sixteen representatives were contacted via email with the questions noted in Chapter 3. Of the sixteen representatives contacted, seven replied with responses to some or all of the questions, one responded that he was not involved in the legislation, and the other eight gave no response. Appendix C summarizes the responses of the seven replying legislators.

The responses given by the state legislators give some interesting insight as to the issues surrounding Smart Card legislation on a state-wide level. The issue of Smart Cards obviously was highly controversial, especially since Representative Brad King

noted that the bill's sponsor, Representative Adair, received threats from ultra-conservative groups. Of the 7 respondents, each were members of the Utah State Legislature during the debates. They were all involved to varying degrees with the bill and with the sponsor Representative Adair. Two of the six representatives noted they had voted against the bill, while the other five voted for it. The results of the vote can be found online at <http://www.shire.net/big.brother/hvotefeb.htm>.

#### 4.4.2 Issues and Voting on the Bill

Various issues prompted both sides of the legislation to vote the way they did. Privacy issues were the most noted concerns. The two representatives voting against the legislation felt that sensitive privacy issues were the main barriers. Representative Harper noted that too much information was available in one place, making the technology an easy target for identity theft. Representative Hunsaker believed privacy was the most significant issue at the time, based on his recollection. Those voting for the legislation believed regardless of privacy issues, the benefits of the technology outweighed the potential problems.

Mixed responses were given as to the factors which allowed the bill to make it through the legislature. Four of the representatives could not remember why, did not respond, or thought the bill did not make it through the legislature. Those who did remember thought it made it through for different reasons. Representative Harper felt that a lack of understanding of the need to keep private information hidden was the reason. Representative Buttars felt that government agencies exerted pressure upon the Legislature to get the bill passed. Representative Buttars opinion seems valid since many of the representatives questioned thought the bill had not passed. Those respondents who

voted against the bill felt the potential problems tied to the technology outweighed the benefits. Representative Brad King felt that potential problems exist, but that the technology to make the information secure exists. Nevertheless, most of the lawmakers who voted for the bill felt that the sensitive information on the cards could be stolen or shared with others.

The extent to which opposition existed against the legislation was made clear by Representative Sheryl Allen's comments. She noted that conservative groups within Utah felt the bill was a major invasion of privacy. Representative Allen also said the bill's sponsor Representative Adair had to have personal protection because his life was threatened by these opposition groups. Clearly, future legislation regarding fingerprint biometric technology similar to the smart card legislation of 1997 would come under heavy opposition from similar conservative groups.

#### 4.4.3 Identity Theft and Privacy Invasion

Based on the results of the questions, it seems the majority of the legislature felt the information contained on the smart cards was highly sensitive and there was great concern over the potential for identity theft. When asked if identity theft was a major concern, all but one of the respondents both for and against the bill felt that it was so. Craig Buttars felt that government access was a greater issue than personal privacy, but the rest of the respondents believed identity theft was a key issue. Representative Sheryl Allen said that the public backlash against the bill was severe and was seen by some as "Orwellian." Regarding privacy invasion, most of the representatives who responded felt that it was a concern. Representative Ralph Becker mentioned that in regard to privacy invasion, there was a mixed response from constituents, but he felt that there appeared to

be adequate protections against privacy invasion. Representative Brad King believed that privacy was a major concern, but that there was not much input from his constituents about it. Representative Sheryl Allen who voted for the bill believed the information on the cards could potentially be stolen. She also mentioned that since the bill had been discussed, identity theft has become a major public issue, particularly after the 9/11 tragedy. Representative Allen also believes that many of her constituents would be willing to have an identity card that would allow them to go through airport security more quickly. Representative Hunsaker did not believe that identity theft was as big an issue as it is today, based upon his recollection.

#### 4.4.4 Summary of State of Utah CIO Comments

In addition to gathering information from legislators, the current Deputy Chief Information Officer for the State of Utah was contacted. Al Sherwood, though not the CIO at the time the Utah Smart Card Drivers License Legislation took place, was able to offer excellent insight as to the issues surrounding the technology.

Mr. Sherwood responded similarly about the groups opposing the legislation. He recalled a right/left-wing coalition which formed that opposed the technology on the basis of privacy issues. When asked about the level of education given to the legislators concerning the technology, Mr. Sherwood believed there probably was not enough given. He also believed that the concerns voiced by the opposition were not properly addressed.

Since the issue of Smart Cards was debated over eight years ago, the question was asked about the possibility of the legislation passing today. Mr. Sherwood was not sure, but he believed that the debate over security and privacy is being played out today over the reauthorization of the Patriot Act. He believes if major concessions were made to get

the Patriot Act reauthorized, opposition to identity management technologies would build strength making smart cards a harder sell. He believes that recent security breaches and the identity theft issues are causing individuals to become more concerned about their privacy than they were before.

#### 4.4.5 Conclusions

Regarding the bill making it to the Senate, the representatives did not think it made it that far. The truth is the bill never made it past the Senate's interim calendar, and similar concerns were voiced to members of the Senate according to the legislature. One of the main opposition groups, according to Representative Brad King, was the Eagle Forum, an ultra-conservative group known for speaking out against privacy issues and controversial identity-management technologies [6]. The life of this bill is an excellent similitude for fingerprint biometric technology. Similar identity management legislation, such as a wide-scale fingerprint biometric application implementation, would likely meet the same opposition in the Utah State Legislature and may never make it into law. Ultra-conservative and other opposition groups would likely make the same arguments and stir up opposition to future fingerprint biometric technology. The identity theft and privacy issues raised by opposition and noted by the representatives are the same types of issues and false perceptions which would need to be overcome through education and training.

The perceptions of CIO Al Sherwood give a further authoritative perspective of the factors limiting the proliferation of Smart Card technology in Utah Driver's Licenses. Privacy concerns are obviously still a major issue, particularly among opposition groups. His comments suggest that there is growing concern over privacy of personal information. Such concern does not bode well for Smart Card technology, and may not



bode well for other new identity management technologies, including fingerprint biometric technology.

The outcome of this legislation is an excellent lesson for states and large organizations considering implementing biometric technology on a large-scale to consider. It illustrates a scenario which could easily recur with another identity management technology such as fingerprint biometric technology. No matter where biometric technology would be implemented, concerns will likely be raised from some part of the user population. Phase III of the research showed that education can overcome some negative perceptions of fingerprint biometric technology. Perhaps if similar education would have been presented concerning Smart Card technology to opposition groups, tempers could have been lessened and the technology would not have been defeated.

## CHAPTER 5 – CONCLUSIONS

### 5.1 Summary of Conclusions

Though automated fingerprint recognition was first developed by the FBI over thirty years ago, the technology clearly is not ubiquitous in industries requiring identity management. Julian Ashbourn, a noted expert in biometric technology said, “...marketable electronic biometric devices have now been around for 15 years or so. Within this time, costs have fallen, matching algorithms have improved, and many suppliers have come and gone – and we are still sitting around talking about emerging technologies. This is a long gestation period.”[27] Fingerprint biometric technology continues to mature, be perfected, and become reliable while simultaneously continuing to come down in price. The present research indicates that the lack of proliferation of this technology is not due to system cost, availability, accuracy, speed, or convenience. Modern fingerprint scanners can be purchased for as little as \$25 bundled with software and drivers and could be adapted to handle more complex identity management needs. Fingerprint biometric hardware is readily available as evident by looking up the technology on Internet search-engines or going to computer-accessory retailers like CompUSA and Circuit City. Benchmark best and worst case false rejection rates (FRR) and false acceptance rates (FAR) of fingerprint verification technology is at .0001-.01% and .3-.7% respectively; and verification speeds of as little as 1 millisecond prove the technology’s accuracy and speed. [24] The technology is obviously convenient and

available—more convenient than existing identity management technologies such as passwords or smart-cards, and is readily available.

This research concludes that user acceptance is the root cause of the lack of presence of fingerprint biometric technology throughout society and commerce. Experts in the field of biometric technology have said: “Fingerprint technology is in the middle of the scale (or low) as far as its acceptance to the general public is concerned. Much of this lukewarm acceptance is due more to perception than reality.”[1]

Research was conducted to understand and evaluate the reasons for poor user acceptance of fingerprint biometric technology. As a technical basis for this research, biometric fingerprint data extraction and template creation was researched. This research was necessary to better understand the process by which most fingerprint biometric systems capture fingerprint data and to use as a tool to educate Phase II respondents on how fingerprint parameter data, but not the actual fingerprint itself, are used. The potential for identity theft by this process is virtually non-existent.

Public domain software produced by NIST for extracting fingerprint minutiae and an inexpensive fingerprint scanner produced by Targus were used to formulate a simple procedure for capturing a fingerprint, extracting the data, and displaying the captured parameters. This technical component of this study contributed to the understanding of the researcher, and the work done in this phase of the study demonstrated how data is extracted from a fingerprint and the type of data used for identifying an individual, the contributor of the fingerprint. This process allowed some respondents involved in the second phase of the research to see how the fingerprint extraction process works and to convince them that only fingerprint parameter data are extracted for identification instead of the entire image.

A significant element of this research involved gaining the authoritative opinion of Utah State law-makers concerning 1997 legislation on implementing smart-card technology as part of the driver's license issuance process. Responses were gathered from as many legislators as possible, and their comments conclude that there were many unanswered questions and concerns over the technology. Opposition was intense and lives were threatened over the legislation. This suggests that a large-scale implementation of a similar identity management tool, such as fingerprint biometrics, would be met by similar opposition. Past successes and failures of identity-capture technology implementations should be taken into account when making identity management technology decisions. For example, the federal government's attempt to establish a federated identity system and the government requiring truck drivers to give their fingerprints should be closely studied to learn about both the problems and solutions experienced, and the degree of acceptance by the population.

## 5.2 Results of Hypothesis

The central hypothesis of this thesis postulates that a population that has received education regarding scientifically established facts of fingerprint biometric technology would exhibit higher levels of acceptance and understanding of the technology and lower levels of concern when compared to the uneducated. The level of acceptance would be measured as a percentage of the surveyed population compared to the level measured previous to education. This hypothesis was based upon two assumptions.

The first assumption was that the non-contributing factors to the lack of fingerprint biometric technology proliferation such as cost, speed, accuracy and convenience had little effect. This assumption appeared to remain valid since the

literature review illustrates the low cost, high speed and accuracy, and the convenience of fingerprint biometric technology.

The second assumption was that misconceptions existed among the population regarding fingerprint biometric technology. This specific assumption appeared to be valid throughout the research since nearly all participants of the surveys held some misconception or misunderstanding concerning fingerprint biometric technology.

The delimitations specified in Chapter 1 of this thesis result in potential areas of bias in this research. The first delimitation specifies that the study was limited to individuals living in Utah, specifically Salt Lake and Utah County. Utah ranks among the leading states in educational attainment of its population. In the year 2000, 90.7% of Utahns over the age of 35 completed high school. Utah also ranked fifth nationally with around 26.9% of Utahns possessing a bachelor's degree or higher. As of 2003, Utah ranked second in the nation for higher education spending and also ranks second in the nation for percentage of households with computers. [29] Since Utah appears to be better educated than many other states in the nation, more accurate and thoughtful responses may have been offered than those which could have been obtained from outside the state.

The second delimitation limited the majority of the surveyed population to individuals working at BYU, Novell, and the Utah State Parks and Recreation office. While all three of these organizations each have several hundred employees and are well-known throughout the State of Utah, individuals from other education, technology, and government offices may have offered different opinions. Individuals from other occupations outside of these three may have differing opinions as well.

The third delimitation specifies the use of demographic information in the two surveys and states that the main purpose for obtaining information about the population's

age, sex, education, and technical expertise was to verify that the population was varied and represented various demographic groups rather than to use in the analysis of the responses. This delimitation helped to assure the surveyed population was varied enough to represent multiple demographic groups.

This hypothesis was tested through the use of two surveys and an online-based fingerprint biometric technology overview, comprising phases two and three of the research. For the second phase of the research, a population of 170 individuals was selected to participate in a survey to determine levels of concern and perceptions of fingerprint biometric technology. This number is in excess of the 150 individuals required for a sufficient sample size. Some of the respondents were shown a demonstration of the technology and the fingerprint extraction process from Phase I to prove that captured fingerprint parameters are used to identify people in a fingerprint biometric system. The results of the survey indicate that there are a number of social issues and false user perceptions which need to be overcome to facilitate user acceptance, at least among the surveyed population.

A number of notable and unexpected revelations arose as a result of the analysis of the Phase II responses:

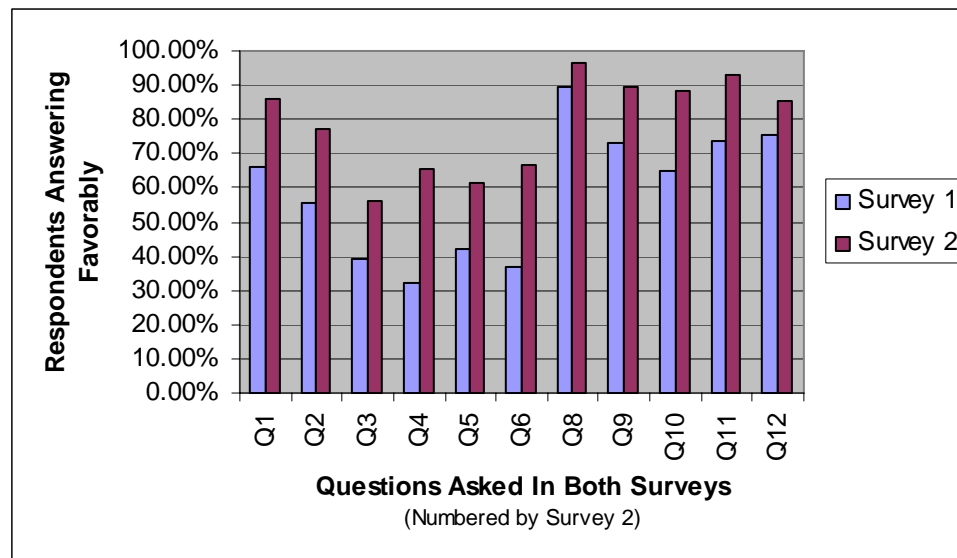
- 1) The majority of respondents thought fingerprint scanning was not an invasion of privacy.
- 2) The majority of respondents believed fingerprint scanning is accurate.
- 3) The legality of fingerprint biometric technology was less of a concern for government workers than for technology or education workers.
- 4) Privacy, third-party data accessibility, and fingerprint image reconstruction was of greatest concern to individuals working in a non-technology occupation.

5) Relating to the question focused on determining the concerns held by the surveyed population, a greater number of concerns were voiced in question 18 than in question 5, indicating a more thoughtful response to question 18.

Since fingerprint biometric technology is not widely used, it was assumed that privacy and accuracy was a predominant concern among the surveyed population. However, the results indicate that neither of these were significant concerns. The legality of fingerprint biometric technology being of lesser concern to government employees compared to employees in education and technology jobs was interesting. An explanation for this can be traced to the greater emphasis on law and legal matters in government settings compared to other industries. Also interesting is the greater level of concern of privacy, third-party data accessibility, and fingerprint image reconstruction among employees of non-technology fields. These results could be explained by the greater technical knowledge commonly possessed by technology workers. Such knowledge would aid understanding of the realities of fingerprint biometric technology and result in lower levels of concern held by the technology occupation segment of the surveyed population. The greater number of concerns from question 18 compared to question 5 was not initially expected, but can be explained. Question 5, which asked about initial concerns surrounding fingerprint biometric technology, was asked previous to questions 6 through 17 – questions which were all related to specific areas of concern. Question 18, which was similar in wording to question 5 but was asked after all of the directed questions on specific areas of concern (questions 6-17), resulted in a greater number of voiced concerns among the surveyed population.

To test the hypothesis of this thesis and to help facilitate user acceptance, an overview of the technology focusing on the facts and strengths of the technology was

created and shared. Of the questions asked in the first survey, eleven of the same questions were asked once more in a second survey. After administering this second survey to 142 of the 170 willing to participate, the results clearly reveal improved understanding gained through the overview significantly changed user perceptions regarding each issue covered as shown below in Figure 4.6.



**Figure 4.6:** Respondents answering favorably in both surveys

As seen in Figure 4.6, each question resulted in more favorable responses after having received the education compared to when the same questions were asked in the original survey. These results illustrate the importance education, through sharing factual information, plays in facilitating positive user perception regarding fingerprint biometric technology. These results also indicate that the stated hypothesis is true. Table 4.1 shown in Chapter 4 illustrates the increases between the numbers of favorable responses from Phase II to Phase III, showing the increases ranged between 7.07% and 33.14%. The average increase in responses between questions from Phase II to Phase III was 19%.



Table 4.2 shown in Chapter 4 also shows the meaningful effect the treatment had upon the Phase III respondents of the survey, clearly showing that education had an effect upon the opinions of respondents. The table showed that each standard deviation in Phase III was less than standard deviations in Phase II, suggesting there were lower variations in responses to the survey questions. Another metric shown in table 4.2 in Chapter 4 is the effect size of Phase II and Phase III. The table shows that questions 4 and 11 have large effect sizes, and questions 1, 3, 5, 6, 9 and 10 indicate medium effect sizes. These numbers indicate the treatment used in Phase III did have a meaningful effect upon responses.

Higher levels of acceptance illustrated by more favorable responses to the survey questions indicate that the surveyed population was favorably affected by the education shared in Phase III of this research compared to previous to the education. It could be concluded that an organization implementing a fingerprint biometric-based identity management system could decrease the numbers of concerns held by a user community thereby increasing the level of user acceptance by educating users prior to system deployment.

### 5.3 Suggestions for Further Study

The present research has identified many areas for continued research which could expand the viability of fingerprint biometric technology and facilitate the results of this study. Further study can and should be undertaken with regard to user acceptance of, and social issues concerning, fingerprint biometric technology. Further research could be conducted in all industries focused upon in this research, namely education, technology, and government. Other industries outside of education, technology, and government,

also could be targeted. Banking and healthcare are large industries that could benefit from the utilization of this technology.

The effect of demographically-targeted education on user perception is another area which could be studied. This research implemented an overview not specifically targeted to individuals of specific age, technological background, occupation, or education. Education targeting specific demographic groups could be performed to determine what elements of fingerprint biometric technology should be stressed for each group to help facilitate acceptance and understanding of the technology.

Another area where little research has been done is the variation in fingerprint biometric viability between different ethnic groups or cultures. Does ethnicity or race play a role in the accuracy and reliability of fingerprint biometric systems? In terms of race, do different physical characteristics exist which would limit the accuracy or reliability of fingerprint biometric technology? Are some cultures more willing and open to using a fingerprint biometric system compared to others? The Mayan culture, currently, commonly uses ink fingerprints for signatures on documents. Cultures with similar practices may accept fingerprint biometric technology more readily than others. Many questions could be asked in relation to fingerprint biometrics and ethnic or cultural factors.

Another area of research could look at the acceptance of ink-based fingerprinting versus digital fingerprinting. Acceptance of these two different methods could help show differences in the perceptions of these methods. One method may seem more intrusive to the population than the other. Understanding these differences could help facilitate solutions and foster acceptance of fingerprint biometric technology.

Though mentioned in the present research, legal issues tied to fingerprint biometric technology could be more thoroughly researched. Individuals such as lawyers and judges involved in first amendment issues could have valuable insight as to the current and future legal issues involved in fingerprint biometric technology. The opinions of these individuals could be gathered and summarized to determine the depth of potential legal problems tied to this technology.

Specific research for facilitating acceptance of fingerprint biometric technology could be performed in the area of feature extraction. Could the number and types of features extracted from fingerprints be varied based upon the size of the population within a limited demographic area? If so, could a ratio of the number of features to the size of the user population be postulated? Such a study could give a better idea and add a level of robustness to the feature selection and extraction process of fingerprint biometric systems.

#### 5.4 Summary

Education can play a role in overcoming false perceptions and positively affecting user perceptions, but it should be understood that a portion of the population will be opposed to any large-scale implementation of fingerprint biometric technology. Whether or not education would affect the perceptions of extreme left or right-wing groups in the political system or other strongly-opposed individuals is unknown, but highly unlikely. To help fingerprint biometric technology become a mainstream identity management solution, the following statement made by the American Association of Motor Vehicle Administrators regarding smart-card adoption should be remembered: “What we need to remember is that most acceptance will come with familiarity of the product. As more

applications become 'visible' to the public, some preconceived barriers will be broken down and less public training and education will be necessary. Being the first to introduce something new is more difficult. Since the public will ultimately bear all or part of the cost of any government application, we must also be made to gain not only public, but also political support.”[20] This comment illustrates the value education has in establishing public acceptance of identity management technology.

Though many areas for further studies exist, the present research has yielded a number of valuable results. The research indicates that a portion of the population in the State of Utah, Salt Lake and Utah counties area including state, education, and technology employees do not fully understand fingerprint biometric technology. Illustrating how the technology works facilitates understanding and acceptance to a certain degree. Education appears to more greatly facilitate positive perceptions of this technology. It remains to be seen how biometric technology might cross the chasm from being an electronic novelty to become a mainstream identity management tool. Biometric fingerprint technology has come a long way in the nearly 30 years it has existed. However, it is evident that fingerprint biometric technology must first overcome significant social barriers before it becomes a conventional identity management technology.



## BIBLIOGRAPHY

1. Chirillo, J., Blaul, S. Implementing Biometric Security. Indianapolis, IN: Wiley Publishing, Inc., 2003: 16, 19, 20-22, 24-25
2. Ashbourn, J. Practical Biometrics: From Aspiration to Implementation. London: Springer, 2004: 28, 30-32, 37-41, 44
3. Woodward Jr, J. D., Orlans, N.M., Higgins, T.P. Biometrics. Berkeley, CA: McGraw-Hill/Osborne, 2003: 64, 198, 201-204, 207, 210, 233, 240
4. Bolle, R.M., Connell, J.H., Pankanti, S, Ratha, N.K., Senior, A.W. Guide to Biometrics. New York: Springer-Verlag, 2004: 130, 139, 146, 153, 161, 212-218, 223, 241-242, 333
5. The Book of Revelation, Chapter 13:16-18. Holy Bible: King James Version.
6. Schlafly P. "ID Card: The Password to the Police State." Eagle Forum Website. 10 Oct 2001. 3 Jan. 2005. <<http://www.eagleforum.org/column/2001/oct01/01-10-10.shtml>>.
7. Ratha N.K., Connell J.H., Bolle R.M. "Enhancing security and privacy in biometrics-based authentication systems." IBM Systems Journal Volume 40 Number 3 (2001).
8. Ahlers, M. "Fingerprinting of Hazmat Truckers Begins." CNN.com. 31 Jan. 2005. 2 Feb. 2005. <<http://www.cnn.com/2005/US/01/31/truckers.fingerprint>>.
9. "Christopher Ann Perkey v. Department of Motor Vehicle"s, 42 Cal. 3d 185; 721 F.2d 50; 228 Cal Rptr. 169 (1986).

10. S. Pankanti, S. Prabhakar, and A.K. Jain. "On the Individuality of Fingerprints." Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition. (2001) : I:805-812.
11. Putte T., Keuning J., "Biometrical fingerprint recognition: don't get your fingers burned." Fourth Working Conf. Smart Card Research and Advanced Applications. Proc. IFIP TC8/WG8.8 (2000): 289-303.
12. U.S. Constitution, 4<sup>th</sup> amendment.
13. "Privacy Act of 1974: 5 U.S.C. § 552a." Department of Justice. 6 Nov. 2004. <<http://www.usdoj.gov/04foia/privstat.htm>>.
14. "Aviation and Transportation Security Act." U.S. Government Printing Office Home Page. 10 Dec. 2004 <[http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=107\\_cong\\_public\\_laws&docid=f:publ071.107](http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=107_cong_public_laws&docid=f:publ071.107)>.
15. Clarke, R. "Human Identification in Information Systems: Management Challenges and Public Policy Issues." Information Technology & People. (1994).
16. "Griswold v. Connecticut" 381 U.S. (1965): 479, 500.
17. "Utility Workers Union of America AFL-CIO v. Nuclear Regulatory Commission" 664 F. Supp. (1987): 138-140.
18. Prindle, P. "Twins and Fingerprints." About.com. 20 Nov. 2003. 4 Mar. 2005. <<http://multiples.about.com/cs/funfacts/a/twinfingerprint.htm>>.
19. Watson, C., Wilson, C. "NIST Special Database 4 Fingerprint Database." NIST Scientific and Technical Databases. 17 Mar. 1992. 6 Mar. 2005. <<http://www.nist.gov/srd>>.
20. American Association of Motor Vehicle Administrators. "Smart Card Usage in Motor Vehicle Administration." (1999).

21. "Results for: Fingerprint" Amazon.com. 3 Jan. 2005. <<http://www.amazon.com/exec/obidos/search-handle-form/002-5883205-0277654>>.
22. Garris, M., Watson, C., McCabe, R., Wilson, C. User's Guide to NIST Fingerprint Image Software. NISTIR 6813. (2001).
23. Moody, J. "Public Perceptions of Biometric Devices: The Effect of Misinformation on Acceptance and Use." Informing Science. 5 Jan. 2004. 31 Jan 2005. <<http://proceedings.informingscience.org/InSITE2004/102moody.pdf>>.
24. Maio, D., Cappelli, R., Jain A. "FVC 2000: Fingerprint Verification Competition." IEEE Transactions on Pattern Analysis and Machine Intelligence, Volume 24 Number 3 (2002).
25. Giesing, I. "User perceptions related to identification through biometrics within electronic business." 25 Mar. 2005 <<http://upetd.up.ac.za/thesis/available/etd-01092004-141637>>.
26. Wilson, C., et al. "Fingerprint Vendor Technology Evaluation 2003: Summary of Results and Analysis Report." National Institute of Standards and Technology. NISTIR 7123. (2004).
27. Ashbourn, J. "Group test one: Biometrics", SC Magazine. Oct. 2004 : 56.
28. McCabe, R. M., "ANSI/NIST-ITL 1-2000 Data Format for the Interchange of Fingerprint, Facial, and Scar Mark & Tattoo (SMT) Information." <[ftp://sequoyah.nist.gov/pub/nist\\_internal\\_reports/sp500-245-a16.pdf](ftp://sequoyah.nist.gov/pub/nist_internal_reports/sp500-245-a16.pdf)>.
29. "Education Overview". Utah Department of Community and Economic Development. 11 May 2005. <<http://relocate2.utah.gov/education>>.



30. Saita, A."ID theft, Phishing Altering Online Habits." SearchSecurity.com. 19 Oct. 2004. 15 Mar. 2005. <[http://searchsecurity.techtarget.com/originalContent/0,289142,sid14\\_gci1017458,00.html](http://searchsecurity.techtarget.com/originalContent/0,289142,sid14_gci1017458,00.html)>

## APPENDICIES



## APPENDIX A

### Survey 1 Questions

1	How many times have you been a victim of identity theft?			
2	To what degree do you consider security more important than convenience?	<i>Security is less important</i>	1.....7	<i>Security is more important</i>
3	How familiar are you with biometrics in general?	<i>Unfamiliar</i>	1.....7	<i>Very Familiar</i>
4	How many times have you used a fingerprint biometric reader?			
5	What concerns do you have about using your fingerprint for identification purposes?			
6	To what degree would you consider fingerprint scanning an invasion of your personal privacy?	<i>Not an invasion</i>	1.....7	<i>Major invasion</i>
7	How easy do you think it is for fingerprints to be stolen or copied?	<i>Difficult</i>	1.....7	<i>Easy</i>
8	After using a fingerprint scanner in a public setting, how easy do you think it would be for your fingerprint information to be stolen or copied?	<i>Difficult</i>	1.....7	<i>Easy</i>
9	After using a fingerprint scanner in a public setting, how concerned would you be about your fingerprint information being distributed, shared, or accessed by a 3rd party?	<i>Not concerned</i>	1.....7	<i>Very concerned</i>
10	Suppose the organization you worked for enforced a policy of fingerprinting each employee. Can this organization legally require you to give your fingerprint?	<i>Doesn't have right</i>	1.....7	<i>Does have right</i>
11	Can a fingerprint image be reconstructed from raw biometric data?	<i>Not Possible</i>	1.....7	<i>Easily Reconstructed</i>
12	To what degree do you have religious or moral objections about using your fingerprint for identification?	<i>No objections</i>	1.....7	<i>Major objections</i>
13	To what degree would you consider using a fingerprint scanner hazardous to your health (i.e. pain, electrical shock, germs?)	<i>Not hazardous</i>	1.....7	<i>Very hazardous</i>
14	How accurate do you think fingerprint scanners are?	<i>Not accurate</i>	1.....7	<i>Very accurate</i>
15	How comfortable would you be with using your fingerprint to enter the building you work in?	<i>Uncomfortable</i>	1.....7	<i>Very comfortable</i>
16	To what degree would you consider a fingerprint more convenient than other security measures? (keycode, password, smart card)	<i>Fingerprint less convenient</i>	1.....7	<i>Fingerprint more convenient</i>
17	To what degree would you consider using a fingerprint more secure than other security measures? (keycode, password, smart card)	<i>Fingerprint less secure</i>	1.....7	<i>Fingerprint more secure</i>
18	Of all the concerns about fingerprints mentioned (privacy, security, legality, morality, accuracy, health) what is your most significant concern with the technology?			

## Survey 1 Data

Job	Age	Sex	Tech	Edu	Demo	questions																	
						1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
E	23	F	Hi	3	Y	0	7	3	0	Security, id theft	1	2	4	6	7	2	1	1	7	7	7	5	Security
E	22	F	Med	3	y	1	6	2	1	Sharing, id theft	4	5	5	4	3	3	1	1	7	4	5	7	Stolen FP, sharing
E	23	M	Low	2	y	0	5	3	0	None	1	2	2	1	7	3	1	1	7	7	7	7	Stolen FP data, data reconstruction
T	40	M	Hi	3	y	0	6	2	1	Accuracy	1	2	2	1	4	3	1	1	5	7	4	5	Accuracy
T	40	F	Hi	2	y	0	7	4	0	Sharing, id theft, copying	1	2	1	4	7	2	1	1	7	7	7	7	Fraud, sharing
T	42	M	Hi	4	y	0	7	3	0	Accuracy	4	2	7	7	1	4	1	1	5	7	5	7	Sharing, stolen FP data
T	22	M	Hi	2	y	0	5	4	0	None	1	2	3	2	7	4	1	1	2	7	6	6	Data reconstruction
E	23	M	Hi	2	y	0	5	1	0	Id theft	4	3	3	3	2	7	1	1	5	6	6	4	Stolen FP, sharing
E	52	M	Hi	4	y	0	6	3	1	None	3	5	4	4	3	5	1	1	5	6	6	5	Privacy, stolen FP
E	28	F	Med	2	y	0	5	1	0	Accuracy	5	3	4	4	6	5	1	1	5	7	6	5	Stolen FP, sharing
E	22	M	Hi	2	y	0	6	1	0	Accuracy, fp damage	4	3	4	4	4	5	1	2	5	6	5	5	Stolen FP, sharing
E	25	M	Med	2	y	0	6	1	1	Privacy, sharing	4	4	5	4	2	3	1	1	6	6	6	2	Sharing, stolen FP data
E	22	M	Hi	2	y	0	4	1	0	Privacy	3	5	7	5	1	6	1	1	6	3	7	4	Privacy, stolen FP
E	25	M	Hi	3	y	0	6	3	0	Copying, sharing	3	2	4	4	7	5	1	1	6	7	6	3	Accuracy, sharing, stolen FP
E	49	M	Hi	4	y	0	4	5	1	Privacy, stolen fp	4	6	6	6	6	3	1	2	6	4	6	4	Accuracy, stolen FP
E	24	M	Hi	3	y	0	5	4	0	Stolen fp	3	5	5	5	4	5	1	2	6	6	6	5	Stolen FP, lost FP
T	28	M	Hi	3	y	0	5	2	0	Data reconstruction, security	1	4	2	2	5	1	1	1	4	6	5	5	Security
T	30	M	Hi	4	y	1	3	4	0	Sharing	2	3	5	3	3	2	1	1	6	4	6	6	sharing
T	42	M	Hi	3	y	0	5	4	1	Accuracy, fp damage	3	3	3	6	2	3	1	1	6	7	2	5	Accuracy, reliability
T	52	M	Hi	4	y	0	5	3	0	None	1	5	2	2	7	2	1	1	5	7	6	7	None
T	43	M	Hi	3	y	0	7	1	0	Stolen fp	3	4	3	6	6	7	1	1	6	5	7	4	Stolen fp, stolen fp data
T	28	M	Hi	3	y	0	6	3	0	Sharing	5	7	2	2	7	2	1	1	5	6	7	6	Security
T	43	M	Hi	3	y	0	6	3	0	Privacy, stolen fp data	6	6	7	7	7	7	1	1	3	6	7	6	Privacy
T	33	M	Hi	3	y	0	6	3	0	Privacy	6	7	5	6	7	7	2	1	4	6	7	7	Privacy
T	23	M	Hi	3	y	0	6	2	0	None	3	7	4	7	7	7	1	2	4	7	7	7	Id theft
T	39	M	Hi	3	y	0	7	2	0	stolen fp	2	6	3	4	7	5	1	1	5	7	7	7	Privacy
T	30	M	Hi	3	y	0	5	3	0	Privacy, stolen fp	5	7	1	4	7	7	1	1	6	7	7	7	Privacy
T	40	M	Hi	3	y	1	6	1	0	Accuracy, id theft	3	2	1	4	1	1	1	1	4	7	7	7	Sharing, id theft, accuracy
T	37	M	Hi	3	y	0	5	6	1	Sharing	3	2	4	5	5	7	1	1	5	7	7	6	Sharing, accuracy
T	42	M	Hi	3	y	0	6	6	1	None	2	1	1	3	6	6	1	1	6	7	7	7	Sharing, stolen FP data
T	43	M	Med	4	y	0	5	7	1	None	1	1	1	1	5	4	1	1	6	7	7	7	None
T	25	F	Med	3	y	0	5	4	0	Copying, id theft	3	6	4	3	6	4	1	1	4	3	3	3	Security, copying, stolen FP data
E	50	M	Hi	5	y	1	4	6	1	None	2	6	2	7	1	1	1	1	4	6	4	4	Security, sharing
E	27	M	Low	2	y	1	6	1	0	none	4	1	2	6	4	7	1	1	6	7	6	6	Reliability
E	27	F	Low	3	y	0	5	1	0	Health(Germs)	1	2	3	5	2	7	1	5	6	7	6	6	Health(Germs), Id theft, reliability
E	21	M	Med	1	y	0	6	1	0	None	1	2	2	3	6	2	1	2	6	6	7	6	Security
E	51	M	Hi	5	y	0	4	6	1	Social Stigma	4	2	2	2	2	2	1	1	6	1	6	5	Social Stigma
T	40	M	Med	4	y	0	7	3	1	Data reconstruction, sharing	1	5	7	4	6	3	1	1	6	7	6	6	Sharing, Data reconstruction
S	68	M	Low	5	n	0	7	2	0	Accuracy, Privacy	3	2	2	5	7	5	2	1	6	7	7	6	Privacy
S	46	M	Low	4	n	1	4	1	0	Privacy	7	2	6	7	7	3	2	2	3	1	1	5	Privacy, sharing
S	64	M	Low	5	n	0	3	1	0	Privacy	3	5	4	7	4	7	1	1	5	4	4	5	Privacy, security
S	56	M	Low	4	n	0	4	1	0	Privacy, id theft, legality	5	4	6	7	1	6	1	2	6	7	6	6	Legality
S	33	M	Med	2	y	0	6	1	0	None	3	2	5	7	3	4	2	1	4	4	3	5	Security
S	47	F	Low	1	n	1	7	1	0	None	1	1	2	3	7	3	1	1	7	7	7	6	Sharing
S	48	F	Hi	2	n	1	5	2	0	stolen fp	2	4	4	5	6	3	3	1	6	7	7	7	Privacy, sharing
S	51	M	Med	4	n	0	6	2	0	Sharing, security	5	3	3	6	6	2	3	1	6	6	6	6	Privacy
S	47	F	Hi	4	y	0	6	3	0		2	1	4	7	7	5	4	3	4	3	1	6	Sharing
S	44	M	Med	1	n	0	6	3	0		0	6	5	5	7	5	2	2	6	6	6	4	Security
S	68	M	Low	3	y	0	4	1	0	Accuracy, Privacy	5	4	4	6	7	4	1	2	4	7	6	6	Accuracy
S	44	M	Low	4	n	0	7	3	0		7	4	7	7	1	5	7	4	7	1	1	4	Privacy
S	32	F	Med	3	n	0	6	1	0	None	2	2	3	4	5	3	1	4	5	6	6	6	Security, Health(Germs)
S	58	M	Low	5	n	0	5	1	0	None	2	3	3	3	7	4	1	1	6	7	7	7	None
S	42	F	Low	2	n	0	7	1	0	Security	1	4	4	4	7	6	1	1	4	7	7	6	Security
S	30	M	Low	3	n	1	6	1	0	None	2	1	3	3	4	3	1	1	6	5	6	7	None
S	66	M	Med	3	y	0	6	3	0	None	2	2	2	2	6	2	1	1	2	7	6	6	None
S	38	F	Low	1	n	0	6	2	0	None	4	2	4	7	6	6	3	5	6	5	6	6	Privacy
S	44	F	Low	3	n	0	7	1	0	None	4	3	6	6	6	7	3	2	6	6	6	6	None
S	36	F	Low	3	n	0	6	3	0	Social Stigma	5	5	5	6	6	1	1	1	4	3	2	4	Accuracy
S	45	F	Med	2	n	0	4	3	0	None	2	5	5	2	7	3	2	2	2	6	6	6	None
S	45	F	Low	1	n	0	7	1	0	None	1	3	5	2	4	2	1	1	6	7	4	5	Health(Germs)
S	63	M	Med	3	y	0	7	1	0	None	1	5	4	7	3	1	1	1	7	7	7	7	Legality
S	55	F	Low	1	n	0	7	1	0	None	1	1	7	7	1	3	1	1	6	7	7	7	Id theft
S	63	M	Low	3	n	1	6	2	0	Stolen fp, finger loss	3	5	5	6	6	4	2	1	6	5	2	4	Security
S	34	F	Low	1	n	0	4	1	0	Privacy	7	4	4	6	4	4	6	4	6	4	4	4	Privacy
T	25	M	Hi	3	n	0	6	5	0	Sharing	4	3	4	6	4	4	3	4	4	3	2	5	Privacy
O	30	F	Low	3	n	0	4	1	0	None	4	3	3	5	1	5	2	1	5	7	7	7	Finger loss
O	25	F	Med	3	n	0	3	1	0	None	1	3	3	3	6	1	1	1	6	7	7	7	Finger loss
O	33	F	Hi	3	n	0	5	2	0	None	1	4	4	4	1	5	1	1	6	6	7	6	Security
O	33	M	Med	3	n	0	3	2	0	Security	4	5	5	5	3	3	1						

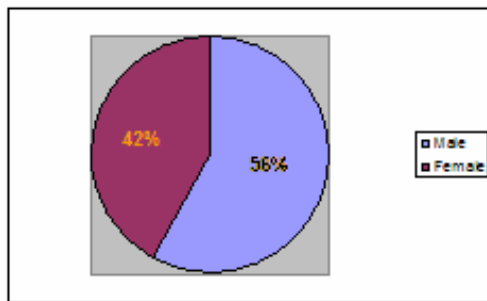
Job	Age	Sex	Tech	Edu	Demo	questions	
T	28	M	Hi	3	n	0 6 4 0 None	2 4 3 4 4 4 3 2 4 6 4 2 None
E	22	F	Low	2	n	0 5 1 0 None	2 2 3 2 7 4 1 1 4 3 4 6 Accuracy
E	20	F	Low	1	y	0 2 1 1 Sharing,privacy	6 4 3 5 1 1 7 4 6 7 Social Stigma
O	26	F	Low	1	n	0 5 1 0 None	1 4 5 4 2 4 2 3 4 3 5 5 Health(Germs)
T	24	M	Hi	2	n	0 6 6 0 None	2 6 6 3 4 6 1 2 6 6 7 3 Security
T	23	M	Med	3	n	1 6 1 0 None	1 4 4 6 1 4 3 1 3 5 7 6 Security
O	22	M	Low	2	n	0 4 1 0 None	3 4 6 5 7 4 1 3 6 5 5 7 Reliability
O	20	F	Low	2	n	0 6 1 0 None	2 2 3 2 6 3 1 1 7 7 5 6 None
O	24	F	Low	2	y	1 5 2 0 Social Stigma	6 4 7 6 4 5 3 2 4 4 3 5 Privacy, security
O	30	M	Low	3	y	0 4 1 1 Security, Social stigma	6 4 6 7 1 5 4 4 3 1 4 4 Privacy
E	22	F	Low	2	n	0 6 1 0 None	2 1 2 3 7 4 1 1 5 6 6 6 Accuracy
E	45	F	Low	3	n	0 6 1 0 Id theft	6 6 6 6 4 6 6 2 4 2 4 4 Security
E	52	F	Low	2	y	0 7 1 0 Reliability	1 7 7 7 7 6 1 1 4 4 7 6 Security
E	57	F	Low	1	n	0 2 1 0 Sharing	6 2 7 7 6 7 7 3 5 1 3 5 Sharing
E	26	F	Low	3	y	0 4 3 0 Id theft	1 5 7 2 5 1 1 1 7 7 7 Id theft
E	20	F	Med	2	n	0 5 2 0 Finger loss	3 3 5 5 4 6 2 1 7 5 7 7 Security
E	23	F	Med	1	n	0 6 5 0 None	3 4 5 6 4 3 2 1 7 5 6 5 Stolen fp data
E	26	F	Low	2	n	0 6 2 0 None	4 1 3 5 2 2 5 2 4 2 6 6 Privacy
E	55	F	Low	2	n	1 7 1 0 None	3 3 7 7 3 3 1 1 3 7 7 7 None
E	30	F	Med	3	n	0 6 1 0 Sharing, id theft	7 7 7 7 4 4 4 1 7 4 7 4 Privacy
E	51	F	Low	2	n	0 7 1 0 None	2 2 3 3 6 3 1 2 6 6 6 7 None
E	27	M	Med	1	n	0 7 4 0 None	5 1 2 5 5 5 1 1 7 7 7 7 Privacy
T	23	M	Med	1	y	0 6 3 1 Stolen fp	2 2 3 3 5 4 1 1 5 3 2 2 Security
T	25	M	Hi	2	n	0 5 3 0 None	1 4 4 7 1 4 1 1 4 4 7 7 Stolen fp
T	22	M	Hi	1	n	0 4 1 0 None	1 5 3 1 1 1 1 1 7 5 6 7 Legality
T	23	M	Hi	1	n	0 5 1 0 None	2 1 5 4 1 1 1 2 5 7 7 6 Accuracy
T	23	M	Hi	1	y	0 7 2 1 Id theft	1 2 1 7 6 4 1 1 4 6 7 7 None
T	21	M	Hi	1	n	1 7 6 2 None	1 1 5 5 3 4 1 1 5 5 6 5 Security
O	24	M	Hi	1	n	0 6 1 0 None	1 2 2 2 1 1 1 1 3 6 7 7 Reliability
T	24	M	Hi	1	n	1 5 5 0 Reliability	5 1 2 2 4 1 1 1 7 6 5 6 Privacy
O	36	M	Med	2	n	1 5 1 0 None	4 2 3 3 4 2 2 6 6 5 5 None
T	21	F	Med	1	n	0 6 1 0 None	1 1 2 3 5 4 1 1 6 3 6 5 Stolen fp
O	21	F	Low	1	n	0 5 3 0 None	3 4 4 4 4 5 3 2 5 5 5 4 Security, Privacy
O	20	F	Low	1	n	0 6 2 0 None	2 4 4 4 1 1 6 2 2 5 2 5 Morality
O	20	F	Med	1	n	0 4 2 0 None	1 2 2 5 5 4 3 1 5 6 6 5 None
T	23	M	Hi	2	n	0 5 2 0 Id theft	3 5 6 7 3 7 1 1 6 2 5 7 Stolen fp
O	22	M	Med	2	y	1 5 1 0 None	3 2 2 5 3 2 1 4 4 6 5 Accuracy
T	25	M	Hi	2	y	0 6 6 1 None	2 1 1 1 1 1 1 1 5 7 7 7 Security, Accuracy
O	20	F	Low	2	n	0 6 2 0 None	2 2 5 3 3 3 2 1 6 6 7 6 Security
O	23	M	Med	3	n	0 6 5 0 None	1 1 2 2 1 4 1 1 7 6 7 7 None
O	19	M	Med	1	n	0 5 1 0 None	2 1 3 7 4 4 3 5 3 3 3 Health(Germs)
O	30	F	Med	1	n	0 6 1 0 Sharing	3 3 5 6 7 2 1 1 6 7 6 6 Security
E	19	F	Low	1	n	0 6 1 0 None	2 1 4 7 1 4 3 5 6 5 6 7 Privacy
O	21	F	Low	1	n	0 6 2 0 Id theft	2 5 4 4 3 3 3 4 4 5 5 Security
O	22	F	Med	1	n	0 6 1 0 None	4 1 3 2 6 4 2 1 5 6 5 6 None
E	29	F	Med	1	n	0 5 1 0 None	1 7 7 4 3 7 2 1 6 5 4 4 Reliability
O	21	F	Low	1	n	0 5 1 1 None	3 1 6 4 3 5 3 2 5 6 6 6 Privacy
E	22	M	Hi	2	n	0 4 1 0 Accuracy	3 2 6 5 7 3 1 1 5 5 7 5 Reliability
O	36					0 7 1 3 None	5 2 3 3 5 1 1 5 5 2 5 None
O	28	M	Hi	1	n	1 6 7 0 None	5 5 5 3 7 7 1 1 6 7 7 7 Stolen fp
E	20	F	Low	2	n	0 5 1 0 None	2 5 5 5 3 3 2 2 5 3 6 4 None
O	20	F	Low	1	n	0 6 1 0 Sharing	5 6 6 5 4 4 1 1 7 5 4 2 Security
E	19	F	Low	1	n	0 6 1 0 None	2 5 5 4 4 4 2 6 5 4 6 4 Health(Germs)
O	24	M	Low	3	n	0 7 1 0 None	1 1 3 3 1 1 1 1 6 7 7 7 Privacy
E	22	M	Med	2	n	0 4 3 1 None	1 1 3 3 5 4 1 1 6 6 5 6 Accuracy
O	29	M	Med	1	n	0 4 1 1 None	1 1 2 2 5 2 1 1 6 7 6 6 Legality
E	21	F	Med	1	n	0 5 1 0 None	4 5 6 6 3 4 2 1 5 4 6 4 Privacy
O	23	M	Hi	1	n	0 6 1 0 None	1 3 3 1 7 7 1 1 7 5 3 7 None
E	21	M	Med	1	n	0 3 2 0 None	2 5 7 2 4 6 2 1 5 4 5 4 Accuracy
O	19	F	Med	1	n	0 5 1 0 None	1 2 1 1 5 2 1 1 3 5 6 5 Accuracy
O	19	F	Low	1	n	0 7 2 0 Id theft	4 5 5 4 1 3 1 1 4 1 1 1 Security
O	20	F	Med	2	n	0 5 2 0 Finger loss	3 3 5 5 4 6 2 1 7 5 4 4 Security
O	23	F	Low	2	n	0 5 3 0 None	1 2 2 1 2 3 1 1 7 4 5 7 Stolen FP data, data reconstruction
O	25	M	Hi	2	n	0 5 3 0 None	1 4 4 7 1 4 1 1 4 4 7 5 Stolen fp
O	26	M	Hi	3	n	0 6 3 0 Copying, sharing	4 2 4 4 3 5 1 1 6 4 6 3 Accuracy, sharing, stolen FP
O	29	M	Low	3	n	1 6 2 0 Stolen fp, finger loss	3 5 5 6 6 4 2 1 6 5 2 4 Security
O	30	M	Low	3	n	0 4 1 1 Security, Social stigma	6 4 6 7 1 5 4 4 3 3 1 4 Privacy
O	31	F	Hi	4	n	1 3 4 0 Sharing	2 3 5 3 3 2 1 1 6 4 6 6 sharing
O	32	M	Hi	1	n	0 5 1 0 None	1 1 5 4 1 3 1 2 5 3 7 6 Accuracy
O	42	M	Hi	3	n	0 6 6 1 None	2 1 1 3 6 6 1 1 6 5 6 5 Sharing, stolen FP data
O	42	F	Hi	2	n	0 7 4 0 Sharing, id theft, copying	1 2 1 4 2 2 1 2 7 4 4 7 Fraud, sharing
O	45	F	Low	2	n	0 6 2 0 None	2 5 5 3 3 5 2 1 6 6 7 6 Security
O	45	F	Low	2	n	0 6 2 0 None	2 2 5 2 2 3 2 2 6 6 4 6 Security
O	56	M	Hi	4	n	0 7 3 0 Accuracy	4 2 7 7 1 4 1 1 5 3 5 5 Sharing, stolen FP data
O	43	M	Med	3	y	0 5 3 0 None	3 2 4 2 3 3 2 1 2 4 4 6 None
O	53	F	Low	1	n	0 6 3 0 None	4 2 4 7 4 5 3 5 4 4 6 4 Privacy
O	29	F	Low	3	n	0 7 1 0 None	5 3 7 5 5 6 3 2 5 6 3 4 None
O	44	M	Med	1	n	0 6 3 0 None	0 6 5 5 2 5 2 2 6 4 4 4 Security
O	68	M	Low	3	y	0 4 1 0 Accuracy, Privacy	5 4 4 6 4 4 1 2 4 4 6 6 Accuracy
O	44	M	Low	4	n	0 7 3 0 None	4 2 3 4 1 5 7 4 2 1 4 4 Privacy

Job	Age	Sex	Tech	Edu	Demo	questions	
O	35	F	Med	3 n	0 6 1 0	Sharing	2 2 3 4 5 3 1 4 5 6 6 6 None
O	31	M	Hi	4 n	1 3 4 0	None	2 3 5 3 3 2 2 1 5 4 5 6 sharing
O	34	M	Hi	1 n	0 5 1 0	None	3 1 4 4 1 3 1 2 5 7 6 7 Accuracy
O	21	M	Low	1 n	0 4 1 0	None	3 3 3 4 2 2 3 2 4 3 3 Privacy
O	22	F	Low	1 n	0 5 2 0	Id theft	4 5 7 5 3 4 5 5 5 5 4 4 Sharing
T	25	M	Med	3 n	1 6 2 0	Copying, Privacy	3 5 3 7 5 4 1 1 7 7 7 7 Security
O	34	M	Med	3 n	0 6 1 0	None	4 2 1 2 1 1 2 2 7 6 6 Legality
O	20	F	Low	1 n	0 6 1 0	Security	1 7 7 6 1 1 1 7 7 7 1 Security
O	20	F	Low	1 n	0 5 1 0	None	5 4 4 7 5 4 1 1 7 4 7 7 Security
E	22	F	Low	2 n	0 5 3 0	Sharing	4 5 5 5 4 4 5 4 4 4 3 3 None
E	25	M	Med	2 n	0 6 2 0	None	1 5 3 5 6 4 1 2 6 6 6 6 Security
E	19	F	Low	1 n	0 5 2 0	Security	2 5 5 4 5 4 3 1 5 4 4 5 Stolen fp
O	21	F	Med	1 n	0 5 1 0	None	4 5 6 6 3 4 2 1 5 4 6 4 Privacy
O	22	M	Med	2 y	1 5 1 0	None	3 2 2 5 3 2 1 4 4 4 5 Accuracy
O	44	M	Low	4 n	0 7 3 0	None	4 2 3 4 1 5 7 4 2 1 4 Privacy
O	25	M	Hi	2 n	0 5 3 0	None	1 4 4 7 3 4 1 1 4 4 5 4 Stolen fp
O	24	M	Low	3 n	0 7 1 0	None	1 2 3 3 1 1 3 1 6 7 4 5 Security

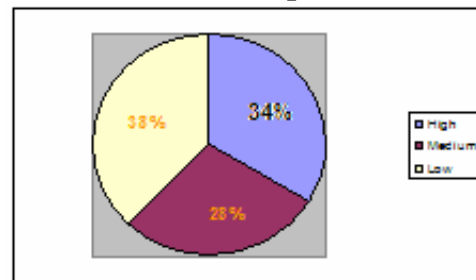
## Demographic Information

### Demographic Information

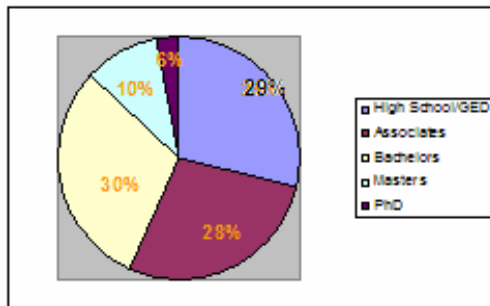
**Gender**



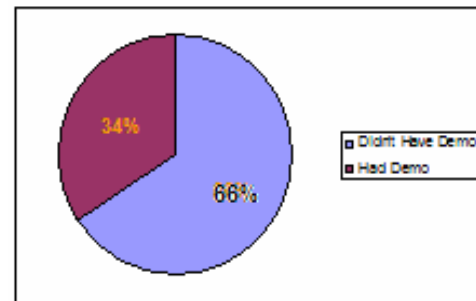
**Technical Expertise**



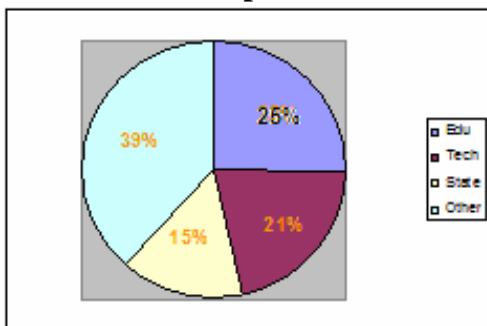
**Education Level**



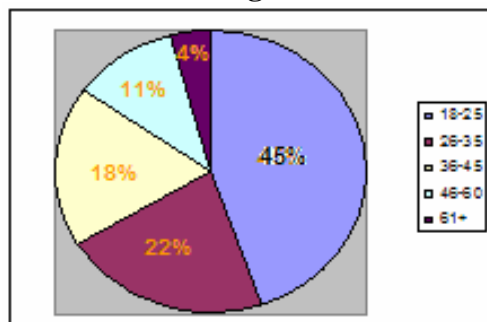
**Received Technical Demonstration**



**Occupation**



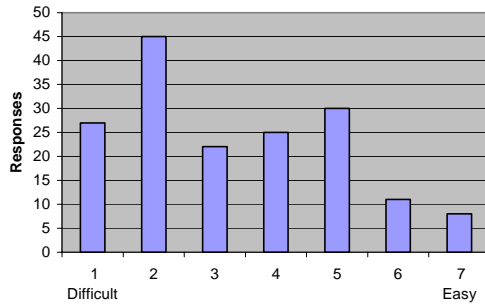
**Age**



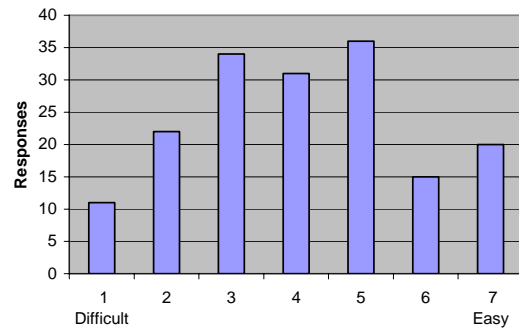




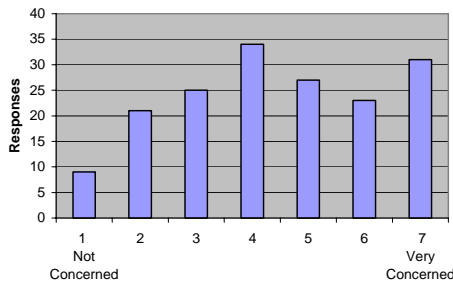
Question 7: How easy do you think it is for fingerprints to be stolen or copied?



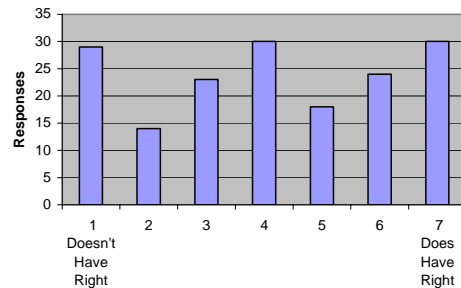
Question 8: After using a fingerprint scanner in a public setting, how easy do you think it would be for your fingerprint information to be stolen?



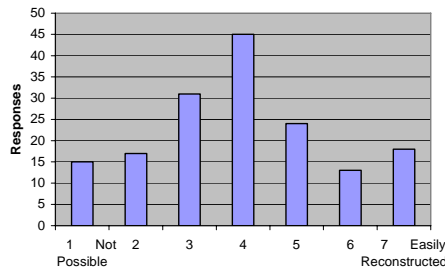
Question 9: After using a fingerprint scanner in a public setting, how concerned would you be about your fingerprint information being distributed, shared, or accessed by a 3rd party?



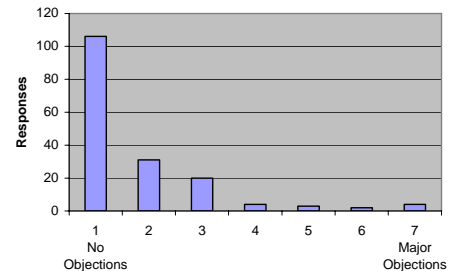
Question 10: Suppose the organization you worked for enforced a policy of fingerprinting each employee. Can this organization legally require you to give your fingerprint?



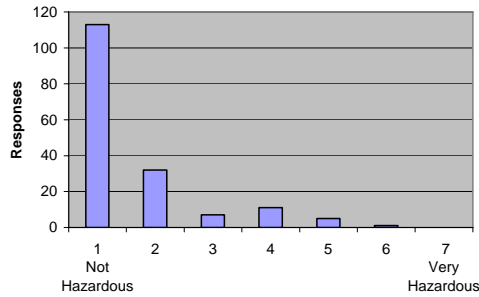
Question 11: Can a fingerprint be reconstructed from raw biometric data?



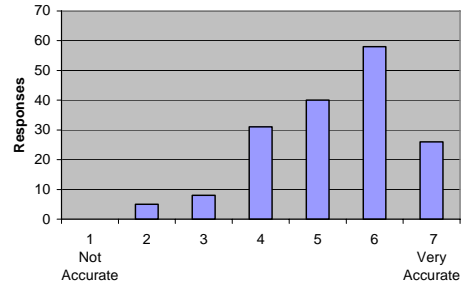
Question 12: To what degree do you have religious or moral objections about using your fingerprint for identification?



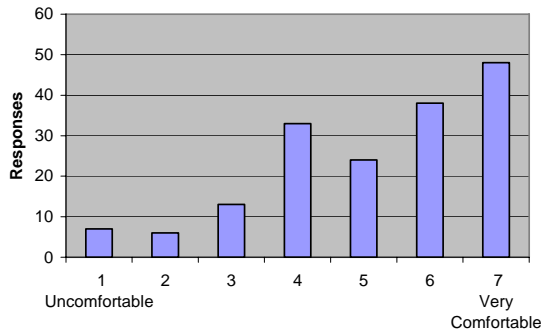
Question 13: To what degree would you consider using a fingerprint scanner hazardous to your health (i.e. pain, electrical shock, germs?)



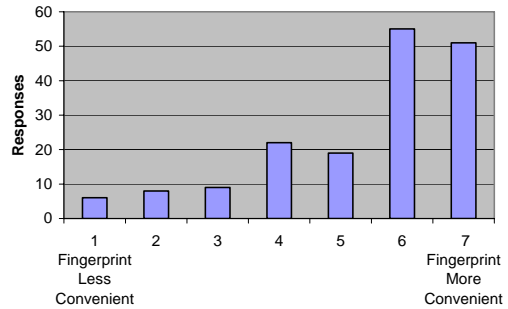
Question 14: How accurate do you think fingerprint scanners are?



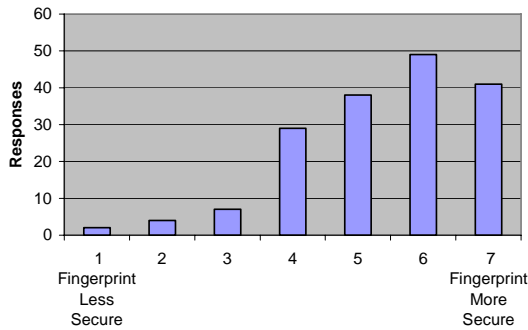
Question 15: How comfortable would you be with using your fingerprint to enter the building you work in?



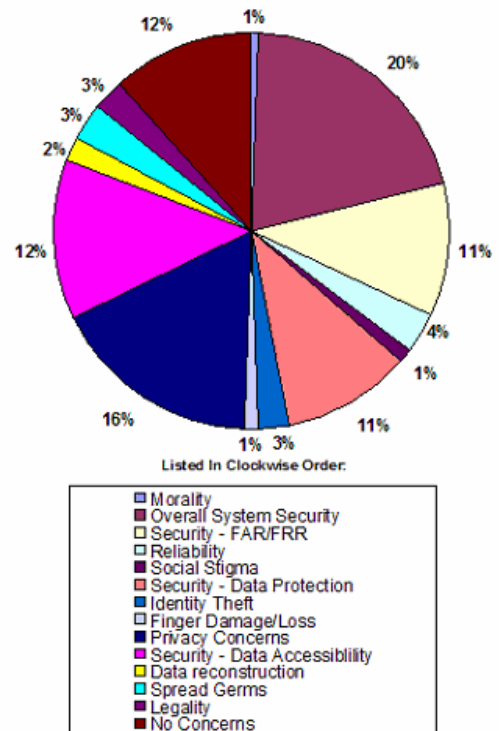
Question 16: To what degree would you consider a fingerprint more convenient than other security measures? (keycode, password, smart card)

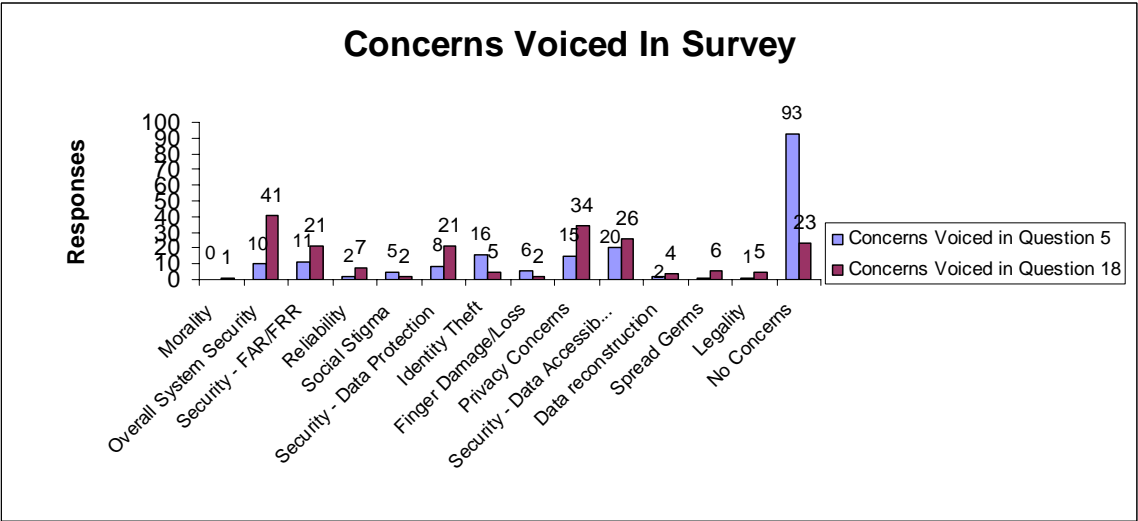
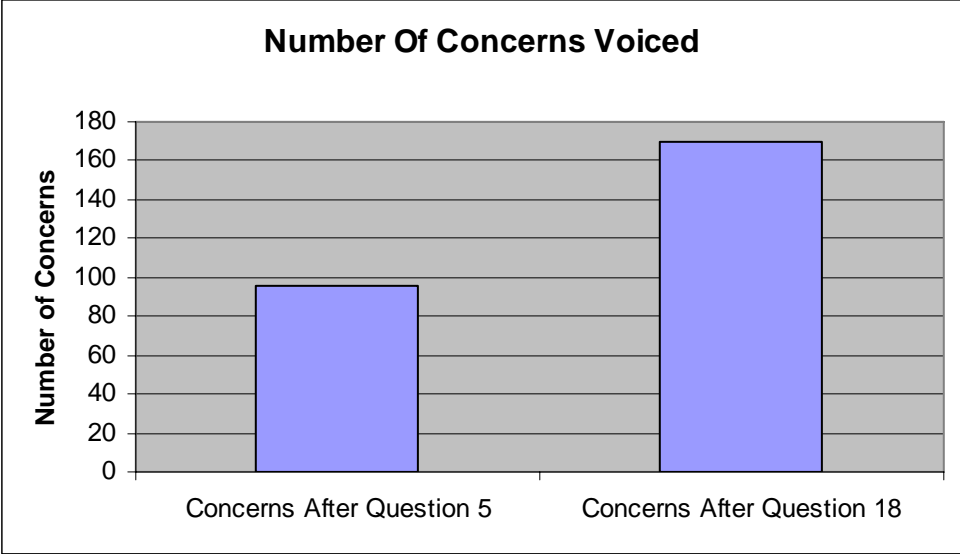


Question 17: To what degree would you consider using a fingerprint more secure than other security measures? (keycode, password, smart card)



Question 18: Of all the concerns about fingerprints mentioned (privacy, security, legality, morality, accuracy, health) what is your most significant concern with the technology?

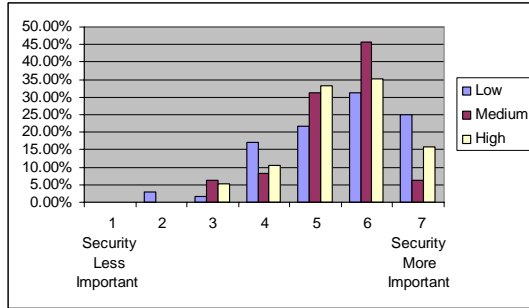




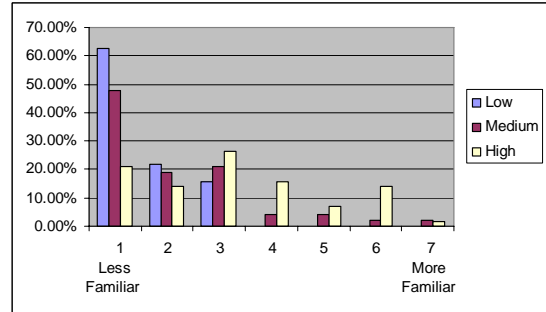
## Results Based on Technical Expertise

### Visual Results Based on Technical Expertise of Phase II Survey

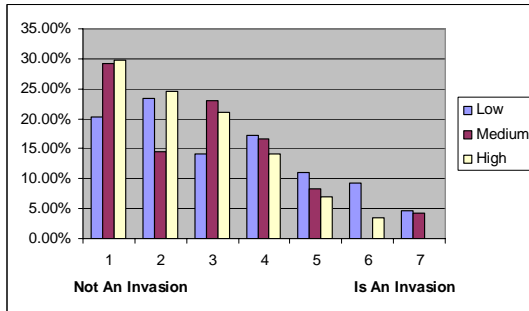
Question 2: To what degree do you consider security more important than convenience?



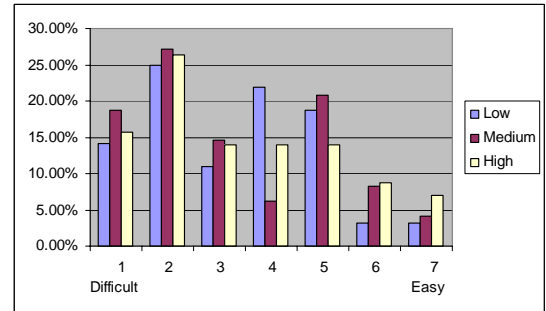
Question 3: How familiar are you with biometrics in general?



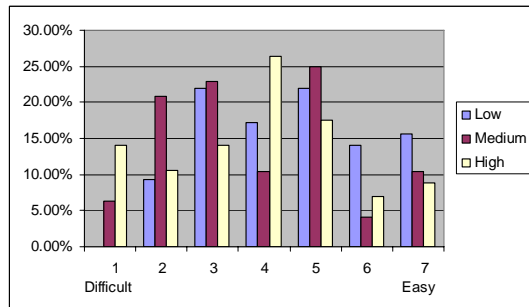
Question 6: To what degree would you consider fingerprint scanning an invasion of your personal privacy?



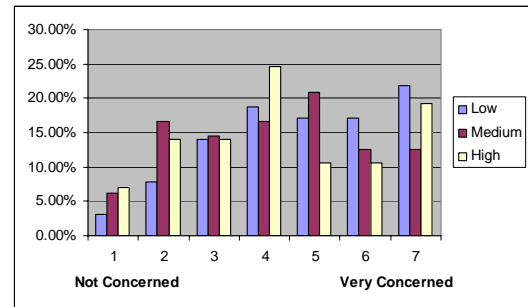
Question 7: How easy do you think it is for fingerprints to be stolen or copied?



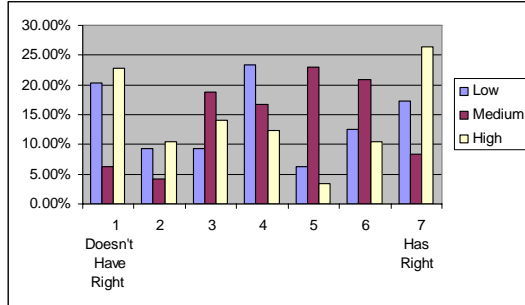
Question 8: After using a fingerprint scanner in a public setting, how easy do you think it would be for your fingerprint information to be stolen?



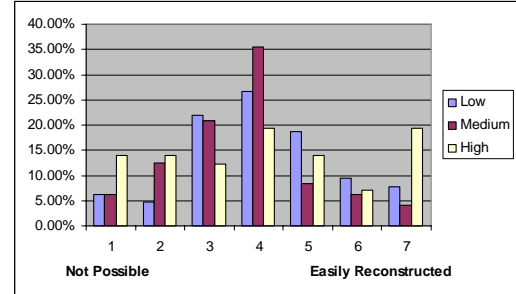
Question 9: After using a fingerprint scanner in a public setting, how concerned would you be about your fingerprint information being distributed, shared, or accessed by a 3rd party?



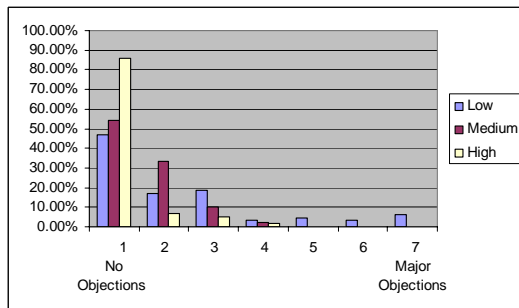
Question 10: Suppose the organization you worked for enforced a policy of fingerprinting each employee. Can this organization legally require you to give your fingerprint?



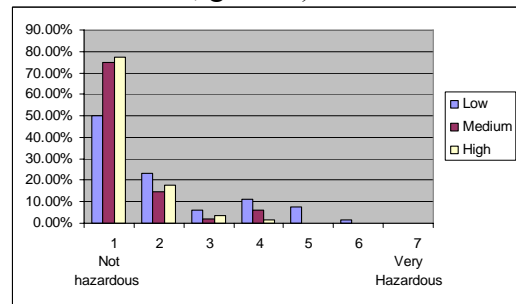
Question 11: Can a fingerprint be reconstructed from raw biometric data?



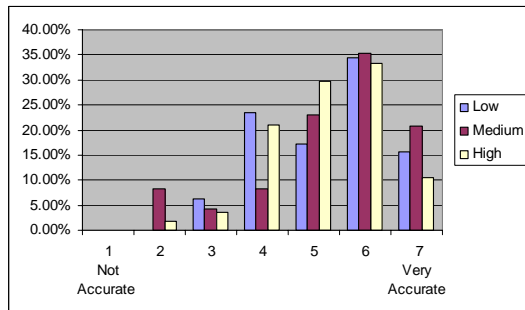
Question 12: To what degree do you have religious or moral objections about using your fingerprint for identification?



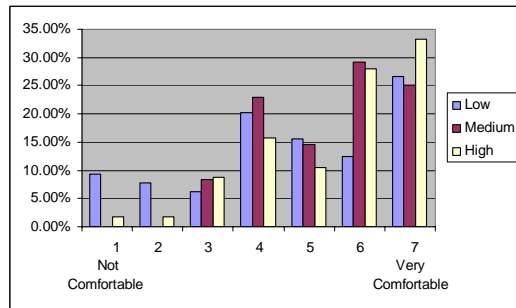
Question 13: To what degree would you consider using a fingerprint scanner hazardous to your health (i.e. pain, electrical shock, germs?)



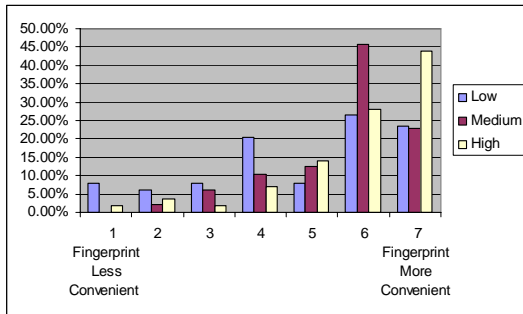
Question 14: How accurate do you think fingerprint scanners are?



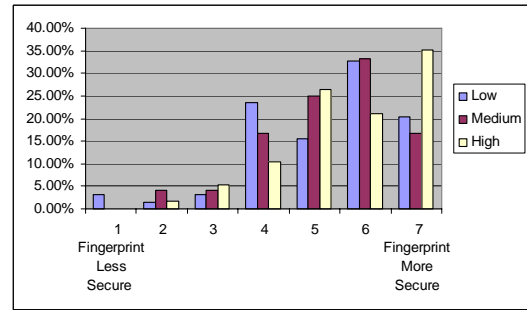
Question 15: How comfortable would you be with using your fingerprint to enter the building you work in?



Question 16: To what degree would you consider a fingerprint more convenient than other security measures? (keycode, password, smart card)



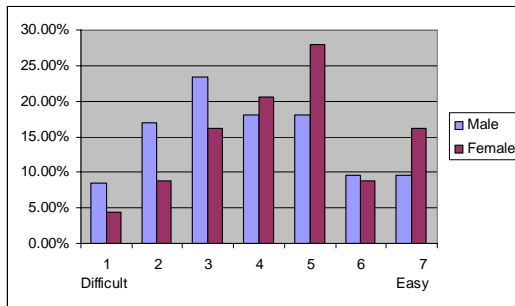
Question 17: To what degree would you consider using a fingerprint more secure than other security measures? (keycode, password, smart card)



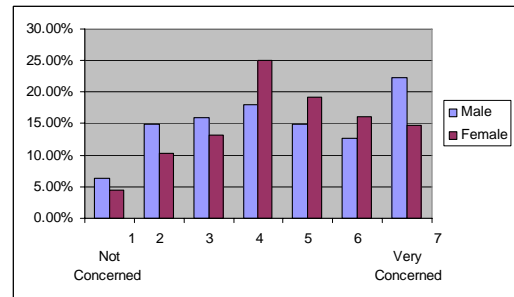
### Results Based on Gender

#### Visual Results Based on Gender of Phase II Survey

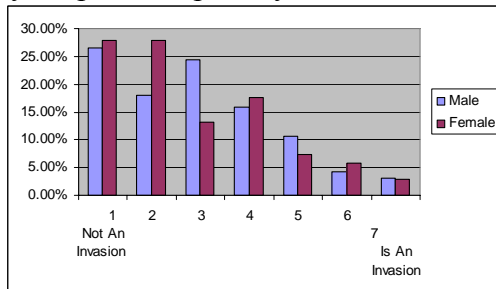
Question 2: To what degree do you consider security more important than convenience?



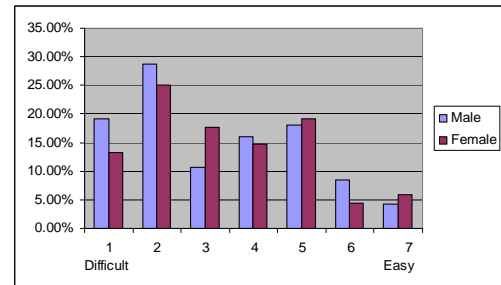
Question 3: How familiar are you with biometrics in general?



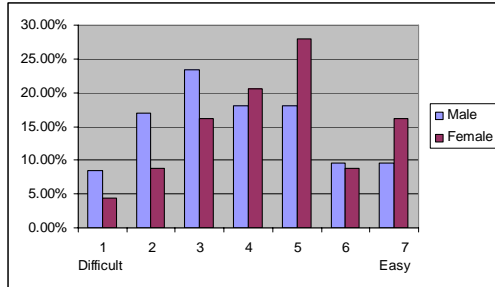
Question 6: To what degree would you consider fingerprint scanning an invasion of your personal privacy?



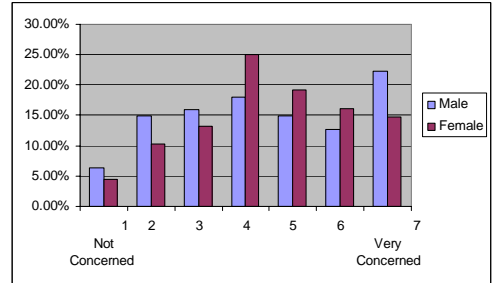
Question 7: How easy do you think it is for fingerprints to be stolen or copied?



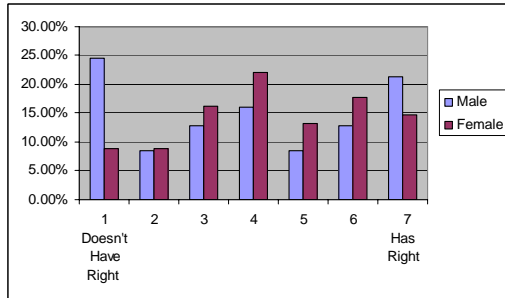
Question 8: After using a fingerprint scanner in a public setting, how easy do you think it would be for your fingerprint information to be stolen?



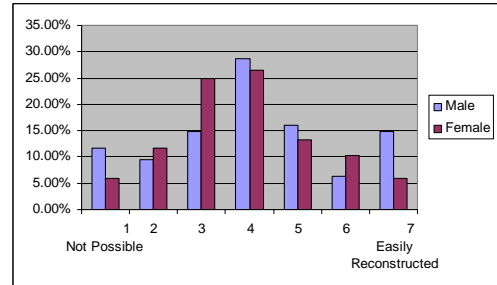
Question 9: After using a fingerprint scanner in a public setting, how concerned would you be about your fingerprint information being distributed, shared, or accessed by a 3rd party?



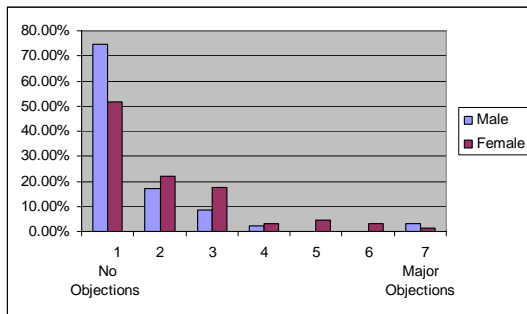
Question 10: Suppose the organization you worked for enforced a policy of fingerprinting each employee. Can this organization legally require you to give your fingerprint?



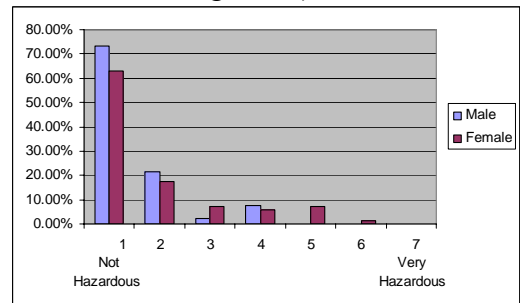
Question 11: Can a fingerprint be reconstructed from raw biometric data?



Question 12: To what degree do you have religious or moral objections about using your fingerprint for identification?

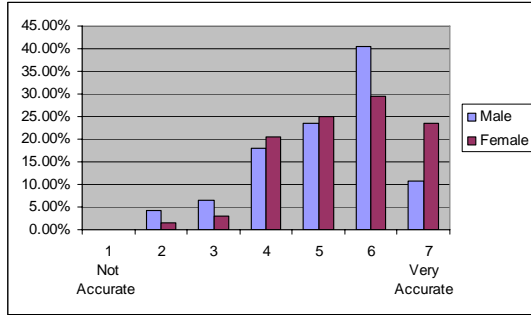


Question 13: To what degree would you consider using a fingerprint scanner hazardous to your health (i.e. pain, electrical shock, germs?)

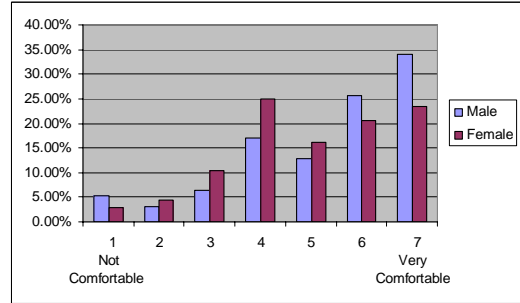




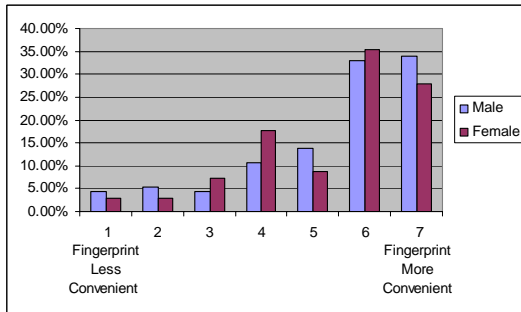
Question 14: How accurate do you think fingerprint scanners are?



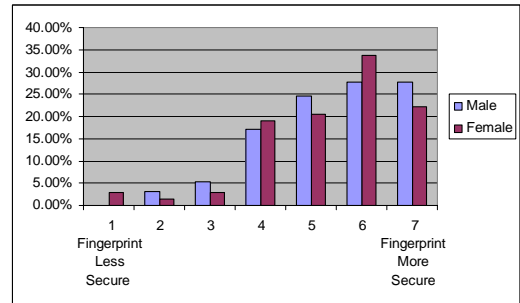
Question 15: How comfortable would you be with using your fingerprint to enter the building you work in?



Question 16: To what degree would you consider a fingerprint more convenient than other security measures? (keycode, password, smart card)



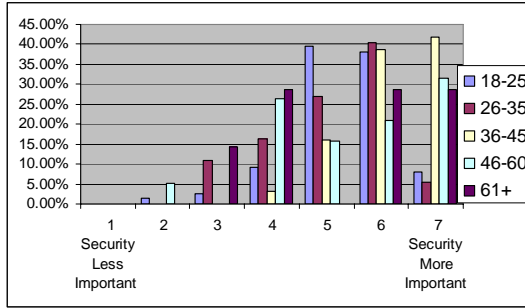
Question 17: To what degree would you consider using a fingerprint more secure than other security measures? (keycode, password, smart card)



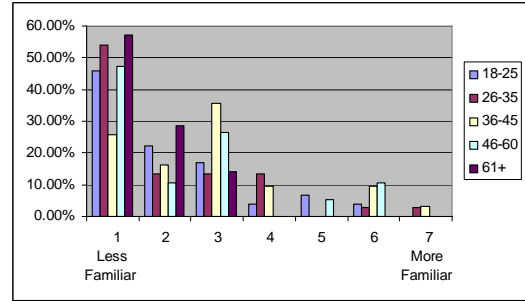
Results Based on Age

Visual Results Based on Age of Phase II Survey

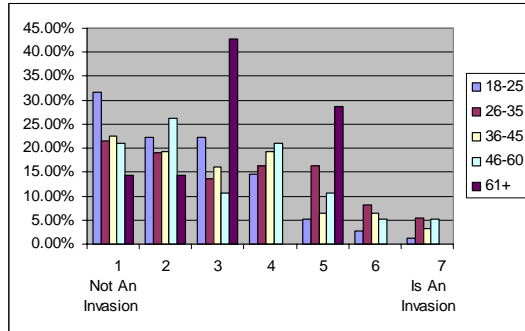
Question 2: To what degree do you consider security more important than convenience?



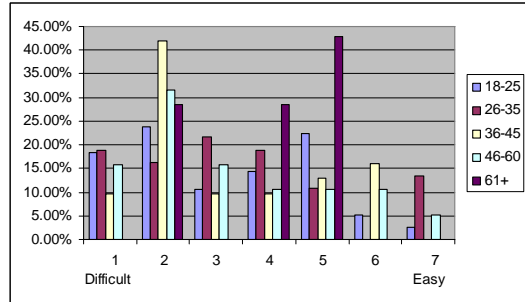
Question 3: How familiar are you with biometrics in general?



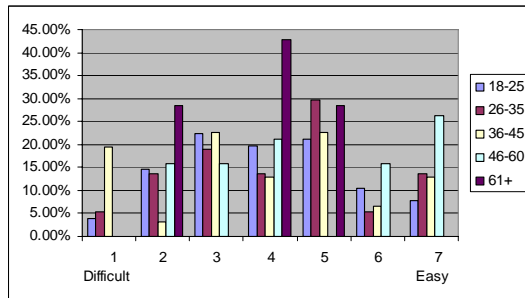
Question 6: To what degree would you consider fingerprint scanning an invasion of your personal privacy?



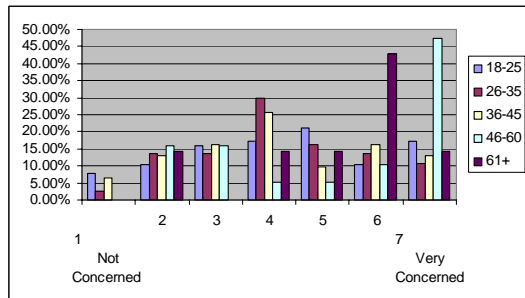
Question 7: How easy do you think it is for fingerprints to be stolen or copied?



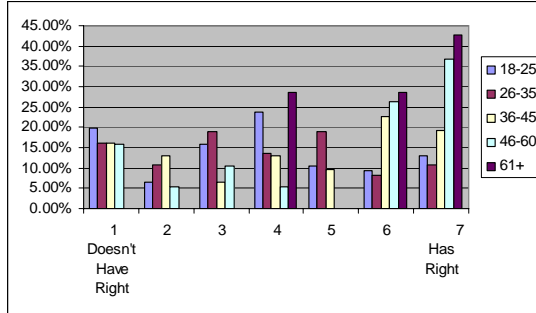
Question 8: After using a fingerprint scanner in a public setting, how easy do you think it would be for your fingerprint information to be stolen?



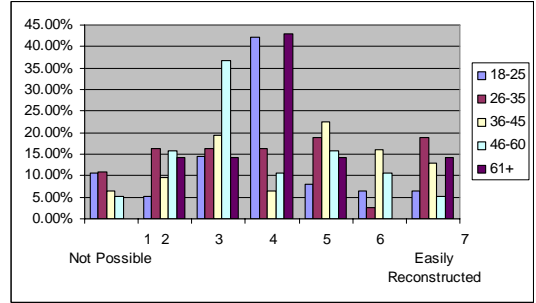
Question 9: After using a fingerprint scanner in a public setting, how concerned would you be about your fingerprint information being distributed, shared, or accessed by a 3rd party?



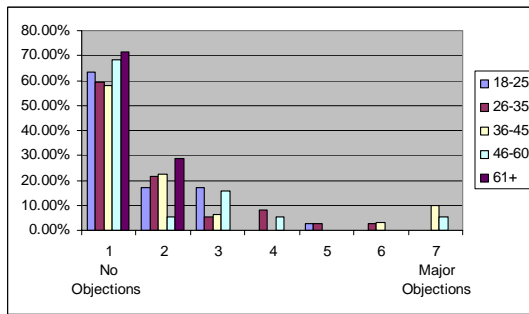
Question 10: Suppose the organization you worked for enforced a policy of fingerprinting each employee. Can this organization legally require you to give your fingerprint?



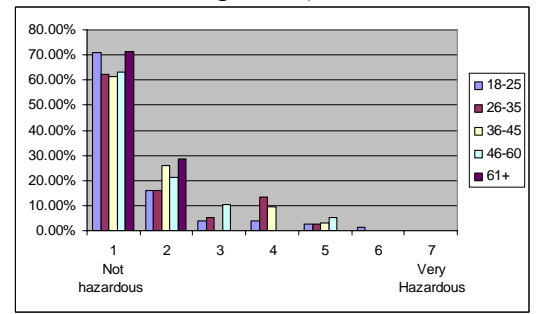
Question 11: Can a fingerprint be reconstructed from raw biometric data?



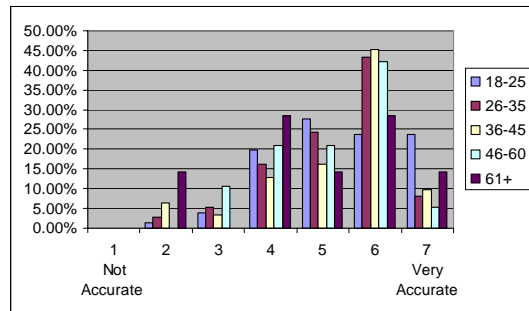
Question 12: To what degree do you have religious or moral objections about using your fingerprint for identification?



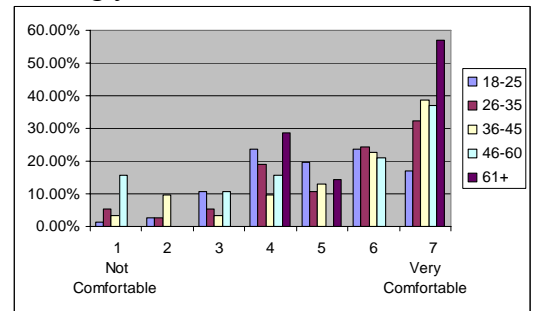
Question 13: To what degree would you consider using a fingerprint scanner hazardous to your health (i.e. pain, electrical shock, germs?)



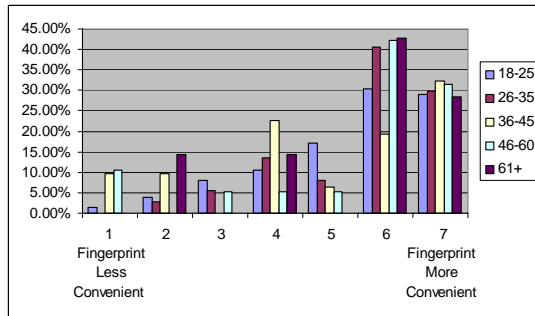
Question 14: How accurate do you think fingerprint scanners are?



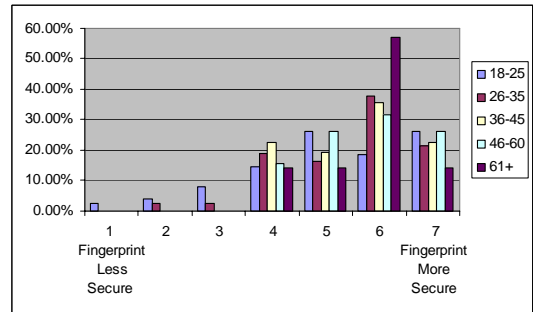
Question 15: How comfortable would you be with using your fingerprint to enter the building you work in?



Question 16: To what degree would you consider a fingerprint more convenient than other security measures? (keycode, password, smart card)



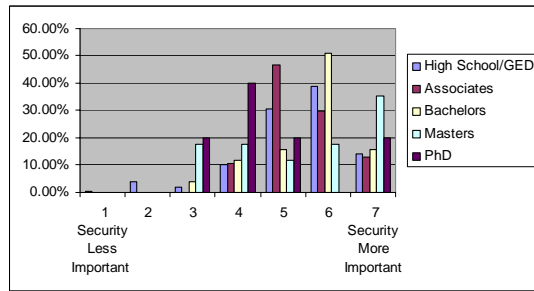
Question 17: To what degree would you consider using a fingerprint more secure than other security measures? (keycode, password, smart card)



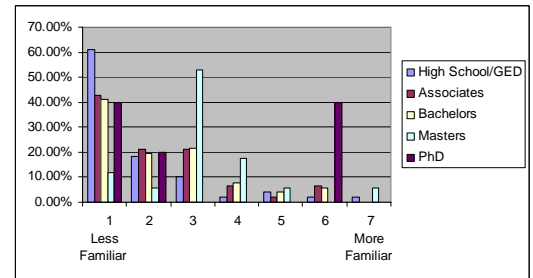
### Results Based on Education Level

#### Visual Results Based on Education Level of Phase II Survey

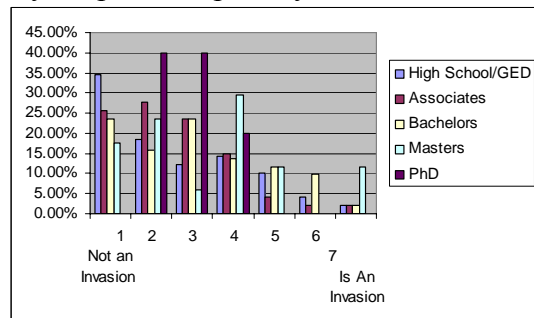
Question 2: To what degree do you consider security more important than convenience?



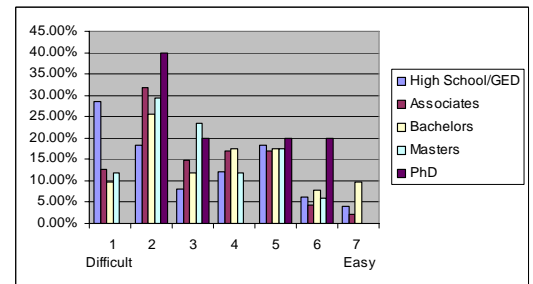
Question 3: How familiar are you with biometrics in general?



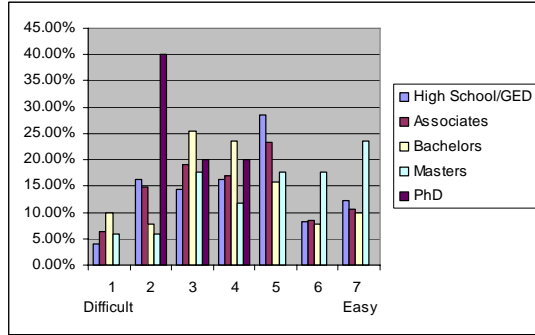
Question 6: To what degree would you consider fingerprint scanning an invasion of your personal privacy?



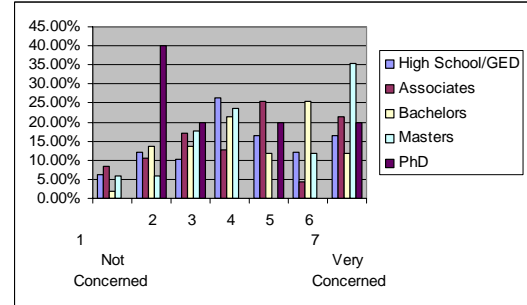
Question 7: How easy do you think it is for fingerprints to be stolen or copied?



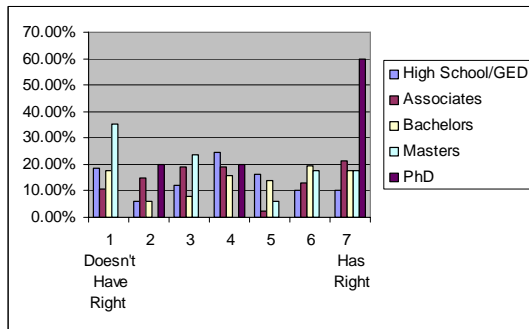
Question 8: After using a fingerprint scanner in a public setting, how easy do you think it would be for your fingerprint information to be stolen?



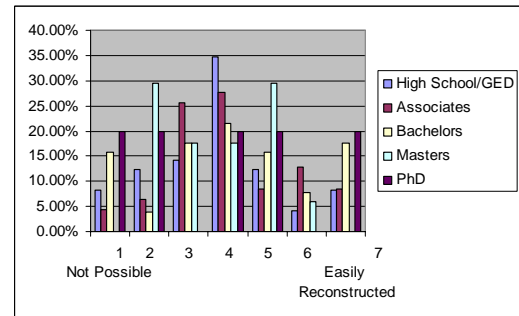
Question 9: After using a fingerprint scanner in a public setting, how concerned would you be about your fingerprint information being distributed, shared, or accessed by a 3rd party?



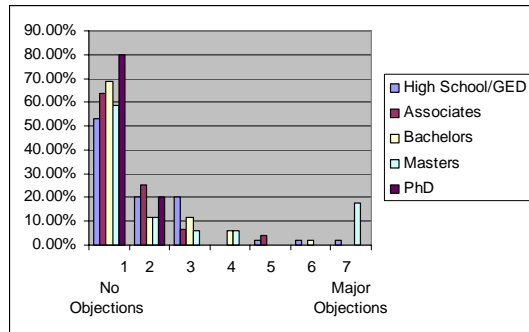
Question 10: Suppose the organization you worked for enforced a policy of fingerprinting each employee. Can this organization legally require you to give your fingerprint?



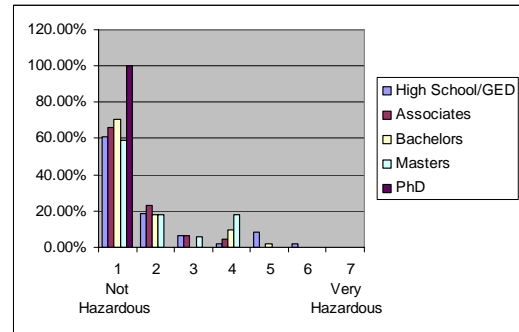
Question 11: Can a fingerprint be reconstructed from raw biometric data?



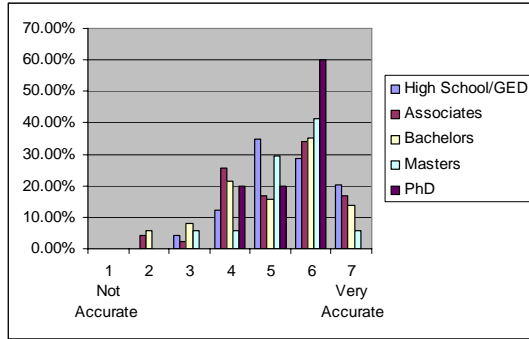
Question 12: To what degree do you have religious or moral objections about using your fingerprint for identification?



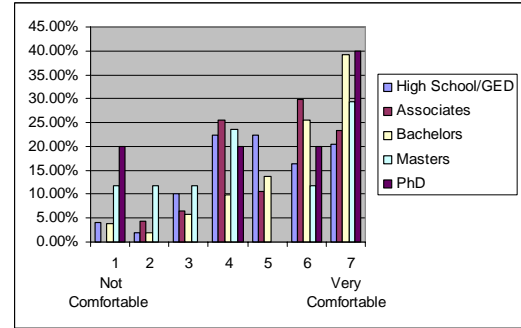
Question 13: To what degree would you consider using a fingerprint scanner hazardous to your health (i.e. pain, electrical shock, germs?)



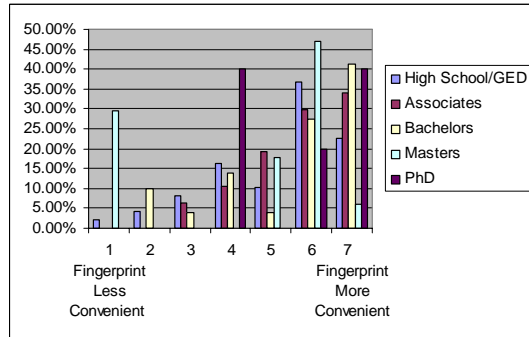
Question 14: How accurate do you think fingerprint scanners are?



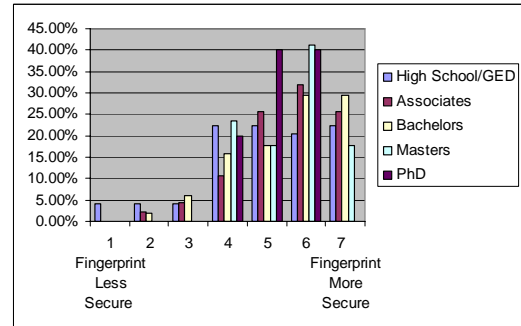
Question 15: How comfortable would you be with using your fingerprint to enter the building you work in?



Question 16: To what degree would you consider a fingerprint more convenient than other security measures? (keycode, password, smart card)



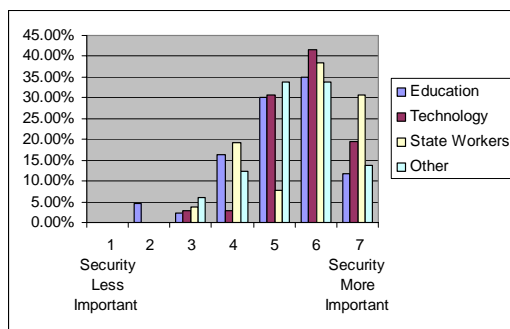
Question 17: To what degree would you consider using a fingerprint more secure than other security measures? (keycode, password, smart card)



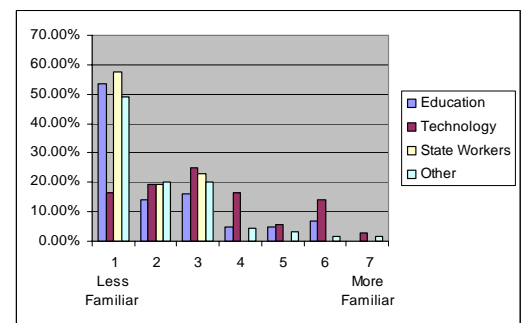
Results Based on Occupation

Visual Results Based on Occupation of Phase II Survey

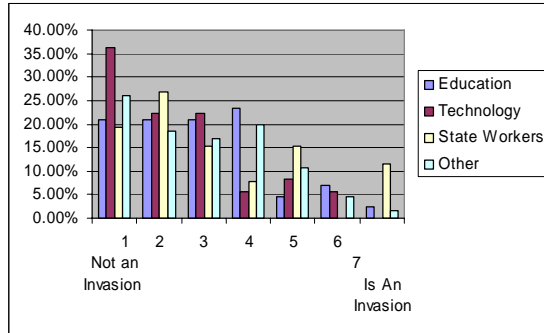
Question 2: To what degree do you consider security more important than convenience?



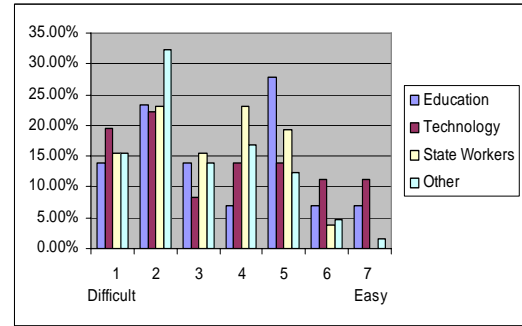
Question 3: How familiar are you with biometrics in general?



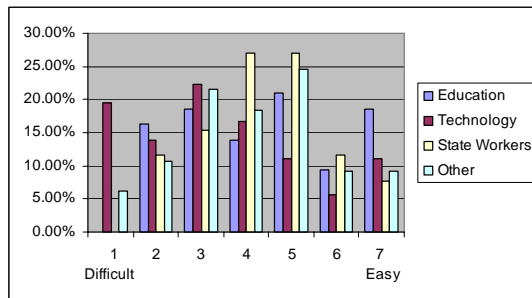
Question 6: To what degree would you consider fingerprint scanning an invasion of your personal privacy?



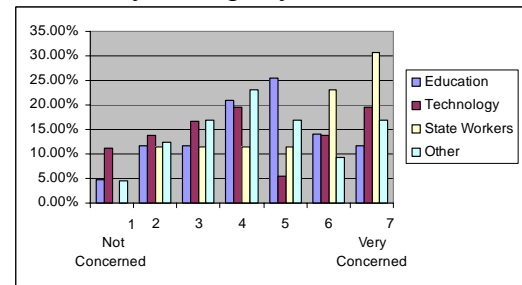
Question 7: How easy do you think it is for fingerprints to be stolen or copied?



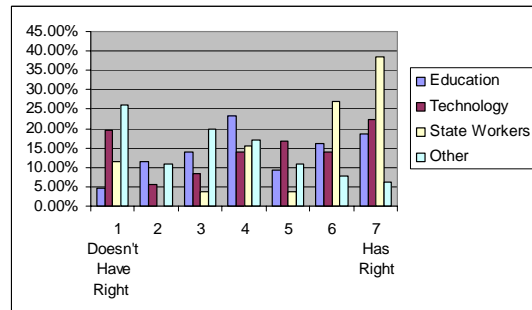
Question 8: After using a fingerprint scanner in a public setting, how easy do you think it would be for your fingerprint information to be stolen?



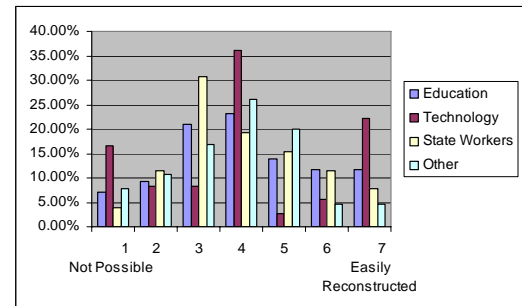
Question 9: After using a fingerprint scanner in a public setting, how concerned would you be about your fingerprint information being distributed, shared, or accessed by a 3rd party?



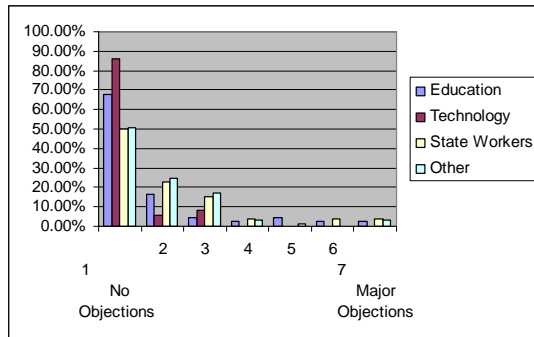
Question 10: Suppose the organization you worked for enforced a policy of fingerprinting each employee. Can this organization legally require you to give your fingerprint?



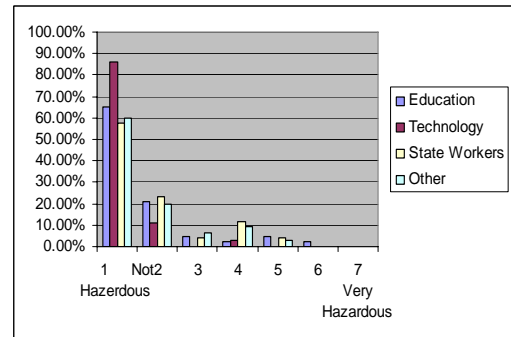
Question 11: Can a fingerprint be reconstructed from raw biometric data?



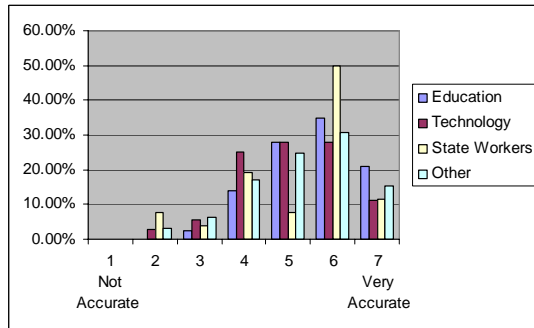
Question 12: To what degree do you have religious or moral objections about using your fingerprint for identification?



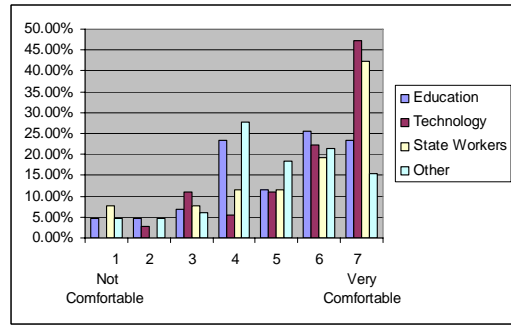
Question 13: To what degree would you consider using a fingerprint scanner hazardous to your health (i.e. pain, electrical shock, germs?)



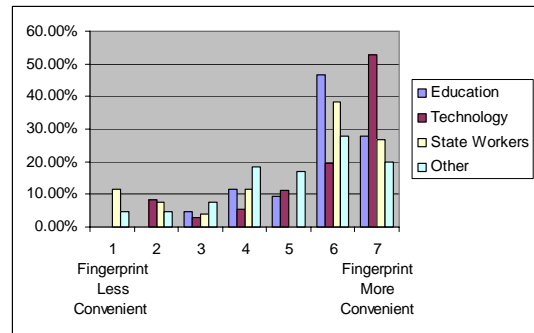
Question 14: How accurate do you think fingerprint scanners are?



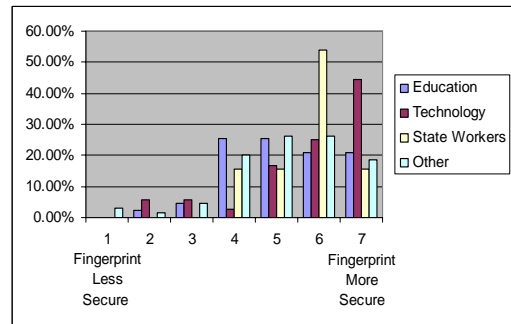
Question 15: How comfortable would you be with using your fingerprint to enter the building you work in?



Question 16: To what degree would you consider a fingerprint more convenient than other security measures? (keycode, password, smart card)



Question 17: To what degree would you consider using a fingerprint more secure than other security measures? (keycode, password, smart card)

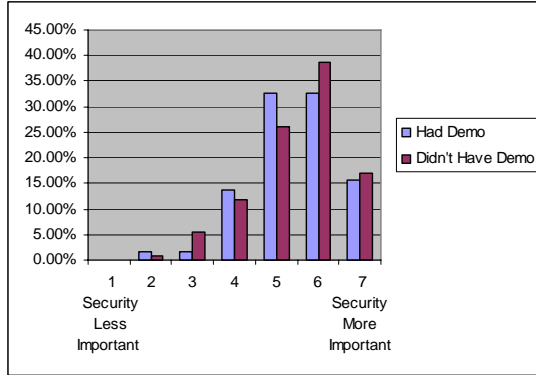




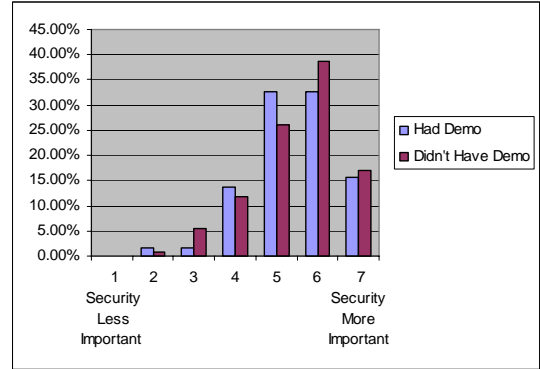
Results Based on Demonstration

**Visual Results Based on Demonstration of Phase II Survey**

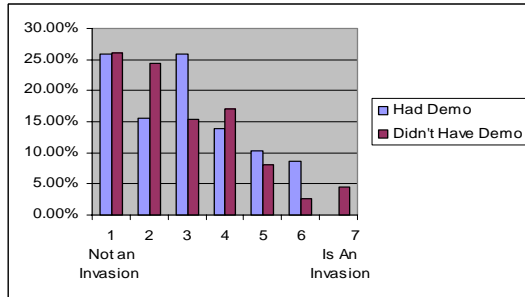
Question 2: To what degree do you consider security more important than convenience?



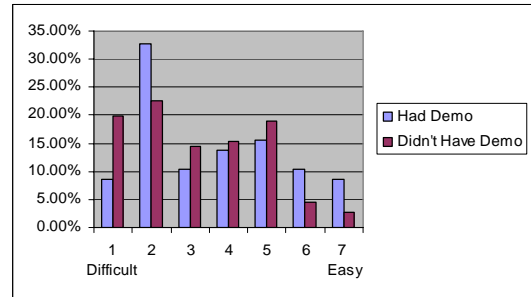
Question 3: How familiar are you with biometrics in general?



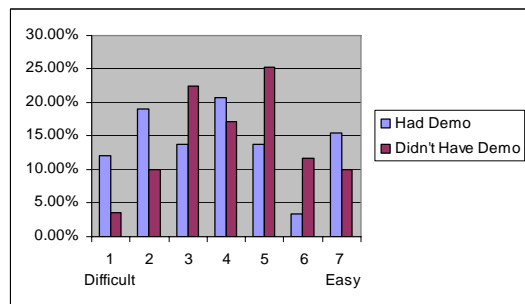
Question 6: To what degree would you consider fingerprint scanning an invasion of your personal privacy?



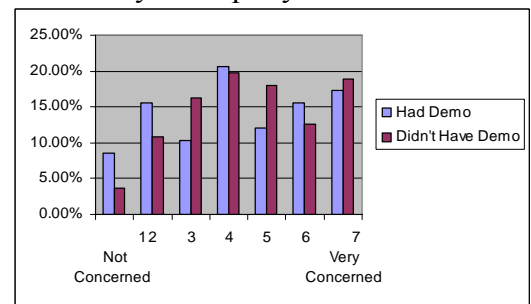
Question 7: How easy do you think it is for fingerprints to be stolen or copied?



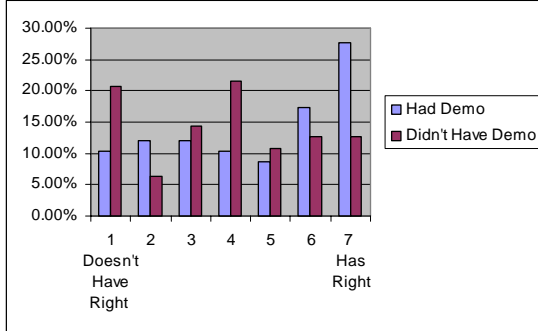
Question 8: After using a fingerprint scanner in a public setting, how easy do you think it would be for your fingerprint information to be stolen?



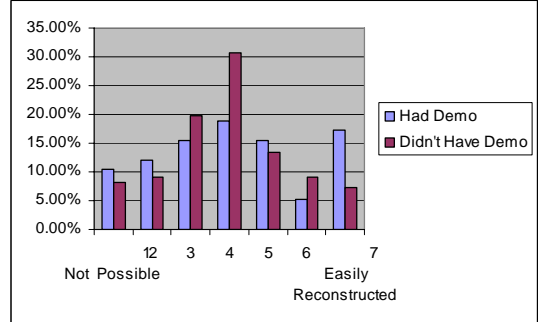
Question 9: After using a fingerprint scanner in a public setting, how concerned would you be about your fingerprint information being distributed, shared, or accessed by a 3rd party?



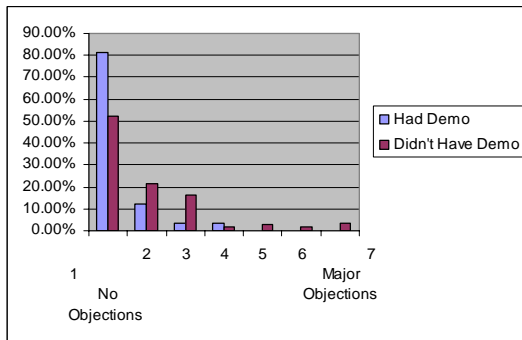
Question 10: Suppose the organization you worked for enforced a policy of fingerprinting each employee. Can this organization legally require you to give your fingerprint?



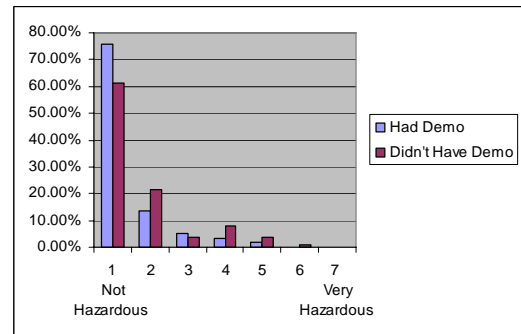
Question 11: Can a fingerprint be reconstructed from raw biometric data?



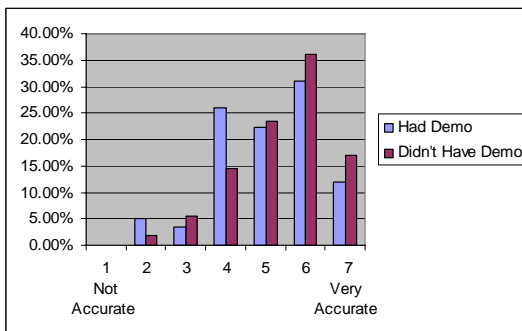
Question 12: To what degree do you have religious or moral objections about using your fingerprint for identification?



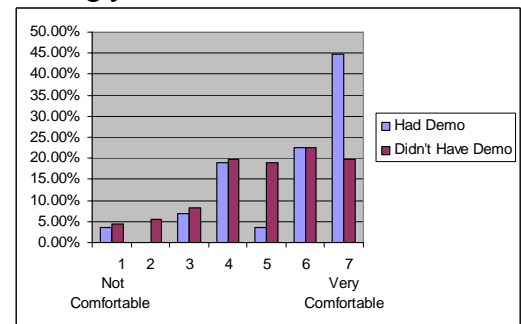
Question 13: To what degree would you consider using a fingerprint scanner hazardous to your health (i.e. pain, electrical shock, germs?)



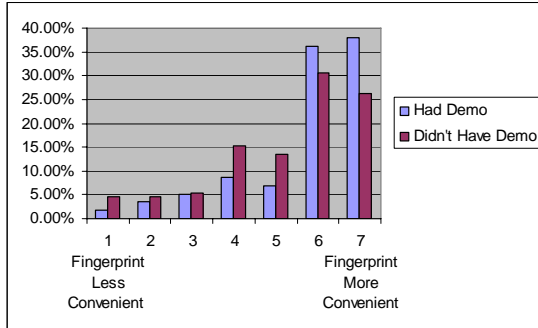
Question 14: How accurate do you think fingerprint scanners are?



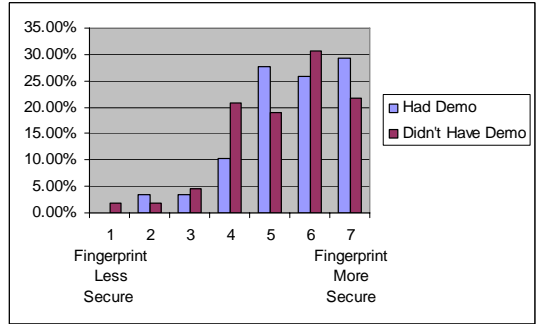
Question 15: How comfortable would you be with using your fingerprint to enter the building you work in?



Question 16: To what degree would you consider a fingerprint more convenient than other security measures? (keycode, password, smart card)



Question 17: To what degree would you consider using a fingerprint more secure than other security measures? (keycode, password, smart card)



## APPENDIX B

### Survey 2 Questions Data

Q 1:	To what degree would you consider fingerprint scanning an invasion of your personal privacy?	Low	1...7	High
Q 2:	How easy do you think it is for fingerprints to be stolen or copied?	Difficult	1...7	Easy
Q 3:	After using a fingerprint scanner in a public setting, how easy do you think it would be for your fingerprint information to be stolen?	Difficult	1...7	Easy
Q 4:	After using a fingerprint scanner in a public setting, how concerned would you be about your fingerprint information being distributed, shared, or accessed by a 3rd party?	Low	1...7	High
Q 5:	Can any organization you work for legally require you to give your fingerprint?	No right	1...7	Full right
Q 6:	Can a fingerprint be reconstructed from raw biometric (electronic) data?	Not Possible	1...7	Possible
Q 7:	To what degree did the previous page reassure you about fingerprint biometrics in general?	Low	1...7	High
Q 8:	To what degree would you consider using a fingerprint scanner hazardous to your health (i.e. pain, electrical shock, germs)?	Not hazardous	1...7	Hazardous
Q 9:	How accurate do you think fingerprint scanners are?	Not accurate	1...7	Very accurate
Q 10:	How comfortable would you be with using your fingerprint to enter the building you work in?	Uncomfortable	1...7	Comfortable
Q 11:	To what degree would you consider a fingerprint more convenient than other security measures(keycode, password, smart card)?	Less convenient	1...7	More convenient
Q 12:	To what degree would you consider using a fingerprint more secure than other security measures(keycode, password, smart card)?	Less secure	1...7	More secure
Q 13:	Having read the previous information, how willing would you be to use a public fingerprint scanner at your place of employment?	Less Willing	1...7	More Willing
Q 14:	Having read the previous information, how willing would you be to use a public fingerprint scanner at a commercial location?	Less Willing	1...7	More Willing
Q 15:	To what degree did the previous page help you better understand how fingerprint scanners work?	Less	1...7	More

## Survey 2 Data

Age	Sex	Tech Exper	Had Demo	Q1	Q2	Q3	Q4	Q5	Q6	Q7	Q8	Q9	Q10	Q11	Q12	Q13	Q14	Q15
NA	M	3	1	4	2	3	2	7	6	5	1	6	6	6	4	4	4	4
19	F	2	0	1	2	3	3	4	6	6	1	7	7	7	7	7	7	7
NA	F	2	0	1	2	4	4	2	5	3	1	5	6	6	6	5	4	3
NA	F	2	0	3	4	4	6	3	5	5	2	5	5	6	5	5	3	6
NA	F	1	0	2	3	3	3	5	4	2	1	6	6	4	6	6	3	4
NA	F	1	0	2	1	1	1	5	2	5	1	6	3	2	6	5	4	5
NA	F	2	0	3	3	4	6	6	2	4	2	6	7	5	5	4	1	6
NA	M	2	0	2	3	5	3	7	2	5	2	6	6	5	5	5	3	5
23	M	2	0	2	5	5	4	4	5	5	1	5	7	5	6	7	6	4
NA	F	2	0	1	4	4	5	4	4	6	3	5	6	7	5	6	6	7
22	F	2	0	5	3	3	6	2	3	4	2	4	6	7	6	5	1	6
20	F	2	0	7	7	7	7	1	5	4	1	7	6	7	5	3	5	5
30	M	1	0	4	2	7	6	4	3	3	2	3	5	6	6	7	7	7
NA	F	2	0	5	2	2	6	3	2	3	5	6	5	4	6	4	2	6
25	M	3	1	2	1	1	2	6	1	7	1	7	7	7	7	7	7	7
NA	M	3	0	1	5	3	2	6	3	4	1	7	7	7	4	5	5	4
22	M	3	1	6	5	5	5	5	6	6	2	5	2	5	5	3	2	5
NA	M	3	0	3	6	3	2	7	7	1	1	6	7	7	3	4	4	5
NA	F	2	0	6	2	4	5	1	3	5	1	7	4	5	5	5	2	6
NA	F	2	1	5	3	5	7	0	4	5	1	6	6	6	6	5	3	6
NA	M	3	1	3	2	2	4	6	3	4	1	6	5	7	4	5	2	4
24	M	1	1	2	2	2	2	6	3	4	1	6	7	7	6	5	5	5
40	M	3	1	1	3	2	3	6	3	4	1	5	7	5	6	5	5	5
NA	M	3	0	3	2	4	2	4	2	6	2	6	5	3	4	5	4	6
22	F	2	1	2	3	2	2	2	4	7	1	7	4	5	6	7	6	7
52	M	3	1	1	2	2	2	6	5	5	2	6	7	6	4	6	6	5
NA	M	3	1	3	2	4	5	6	1	5	2	7	6	7	6	6	5	5
29	M	3	1	2	2	2	3	5	1	6	1	6	7	5	5	6	5	7
43	M	3	1	3	6	5	4	6	2	3	1	7	5	4	5	3	3	6
27	M	2	1	3	2	3	3	4	3	5	1	6	6	6	6	6	5	4
28	M	3	1	4	2	2	5	1	6	5	1	6	5	6	5	4	3	6
39	M	2	1	2	3	4	7	1	1	5	1	5	6	6	7	6	2	6
39	M	3	1	3	4	4	2	4	2	5	2	6	6	6	6	6	6	5
27	F	2	1	6	4	5	5	4	2	5	2	6	6	7	6	6	5	6
27	M	2	1	3	2	2	2	4	3	5	1	7	7	7	7	7	6	6
43	M	3	1	1	2	2	1	7	2	1	1	6	7	7	7	7	7	4
38	M	3	0	1	1	1	2	6	7	7	1	7	7	7	7	7	5	7
68	M	2	1	2	1	4	2	7	2	6	1	7	6	7	7	6	6	7
NA	F	2	1	3	4	5	5	5	5	5	1	6	5	6	0	4	3	5
NA	F	2	0	1	2	2	1	4	1	6	1	6	7	7	7	7	7	7
48	F	2	0	1	3	3	3	6	3	6	1	6	7	7	7	7	6	7
NA	M	1	0	2	1	2	2	7	6	6	2	6	7	7	6	4	4	6
32	F	2	0	2	2	4	1	2	4	6	4	6	5	6	7	6	3	6
44	F	2	0	2	1	2	2	7	1	7	2	6	6	7	7	7	7	7
30	M	1	0	2	1	3	2	1	2	5	2	6	6	7	6	6	5	3
44	M	1	0	3	5	4	5	6	7	5	1	5	7	7	4	6	4	6
48	F	1	0	1	1	3	3	4	5	4	1	5	6	6	6	6	6	4
45	F	2	0	2	2	2	2	2	3	2	6	6	6	6	6	6	5	6
NA	F	1	0	2	3	4	6	5	4	5	2	5	5	6	6	6	6	6
24	M	3	0	1	2	5	4	7	6	5	2	7	7	7	6	6	2	5
55	F	1	0	1	2	3	4	3	2	2	2	3	3	4	4	3	2	3
25	M	2	1	1	2	5	2	6	5	5	2	6	7	6	4	6	6	5
21	M	1	1	2	2	2	2	6	3	4	1	6	7	7	6	5	5	5
29	M	3	1	3	4	4	4	1	7	4	1	4	7	7	4	7	7	4
NA	M	3	1	3	4	4	5	6	6	6	1	6	6	5	6	6	5	5
40	F	2	1	3	1	2	3	7	4	4	1	6	7	7	7	7	6	5
NA	M	3	1	2	3	3	3	7	4	5	2	6	7	7	5	6	4	6
NA	M	3	1	4	4	4	4	6	5	4	1	5	6	6	6	6	4	4
34	F	1	0	5	2	2	2	5	2	5	1	7	4	7	7	4	4	6
43	M	3	1	4	2	2	6	6	5	5	1	6	6	6	6	6	4	4
22	F	2	0	1	1	5	1	7	1	6	1	6	7	7	7	7	7	5
53	F	2	1	1	1	1	1	7	1	7	1	7	7	7	7	7	7	7
NA	M	2	0	2	2	3	3	2	2	6	1	6	6	6	6	6	6	5
20	F	2	0	2	2	3	1	6	2	4	1	7	5	7	6	5	4	7
NA	F	1	0	7	3	6	6	1	1	4	1	7	1	6	6	1	1	7
23	F	1	0	3	3	4	4	1	1	5	1	7	5	7	7	5	5	6
22	M	3	1	1	2	2	1	7	2	6	1	7	7	6	7	7	7	7

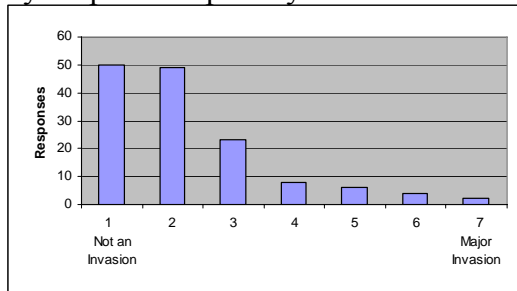
Age	Sex	Tech Exper	Had Demo	Q1	Q2	Q3	Q4	Q5	Q6	Q7	Q8	Q9	Q10	Q11	Q12	Q13	Q14	Q15
66	M	2	0	1	1	1	2	6	2	6	2	6	7	7	7	7	6	7
33	M	2	0	2	3	2	4	5	2	4	2	5	5	5	5	5	5	5
NA	M	3	0	2	2	3	3	7	6	5	2	6	6	6	6	6	5	5
51	F	2	0	1	1	2	2	6	5	6	3	6	7	6	6	6	3	7
57	M	2	0	6	2	3	7	6	4	4	1	7	4	4	7	4	2	4
NA	M	2	0	5	3	4	6	5	3	6	2	5	5	6	6	4	2	7
NA	M	2	0	1	4	7	7	7	4	4	1	6	7	0	6	4	4	5
NA	F	1	0	3	2	6	2	1	2	6	5	6	4	5	4	5	5	6
25	M	3	0	1	3	1	1	7	1	5	1	5	6	7	6	6	4	5
21	F	2	0	2	3	3	2	4	2	4	1	4	6	5	5	5	4	6
NA	F	1	0	1	3	5	3	5	2	1	1	7	7	7	7	4	1	4
23	M	3	0	1	1	3	2	6	2	7	1	7	7	7	7	7	7	7
NA	F	1	0	4	5	1	2	7	5	5	3	7	3	7	7	4	5	6
24	M	3	0	1	3	2	1	7	2	6	1	6	7	7	7	7	5	6
NA	F	1	0	1	1	2	2	6	2	7	1	7	6	7	6	7	6	7
NA	F	1	0	3	3	4	3	5	5	6	2	6	5	5	6	5	4	4
NA	M	2	0	1	1	2	3	6	2	6	1	7	6	6	7	7	7	6
NA	F	2	0	4	4	4	5	6	2	6	1	5	5	6	6	6	6	6
NA	F	2	0	2	2	3	2	3	2	6	1	6	7	7	7	7	5	6
51	F	2	0	2	2	2	3	7	4	0	1	6	6	5	6	6	5	7
30	F	1	0	5	4	2	2	4	2	6	1	6	4	6	6	3	3	7
NA	F	2	0	4	2	6	4	2	3	3	1	0	3	4	4	5	2	4
NA	F	1	0	1	4	2	2	3	1	6	1	7	6	7	5	7	4	7
NA	M	2	0	2	2	5	4	5	2	7	2	6	7	7	5	5	4	6
NA	M	2	0	1	1	6	2	5	1	7	2	6	7	7	4	6	4	7
25	M	0	0	3	2	4	4	6	1	7	1	6	5	6	5	7	3	7
NA	M	3	0	1	5	4	2	7	2	6	2	7	4	7	4	5	4	7
NA	F	1	0	2	3	4	3	4	2	5	3	6	7	5	6	6	5	6
NA	F	1	0	2	3	7	6	4	3	6	6	7	6	5	4	6	4	7
NA	M	2	0	3	1	6	3	4	4	5	1	7	7	5	7	5	5	7
NA	M	1	0	2	4	5	2	7	2	6	1	6	5	6	6	4	3	7
NA	F	1	0	1	1	5	6	5	1	7	1	6	6	5	4	6	5	7
22	M	3	0	1	3	4	4	5	6	5	1	7	5	7	6	5	3	6
NA	M	3	0	2	2	2	4	3	2	6	1	6	6	5	4	7	6	5
NA	M	3	0	1	2	6	3	4	1	7	2	5	6	6	5	7	3	6
NA	M	3	0	1	1	2	2	6	2	7	1	6	6	7	5	3	4	7
NA	M	3	0	1	2	1	2	6	1	6	1	6	7	7	5	7	5	7
NA	M	3	0	3	1	6	2	7	1	7	1	7	7	6	6	5	4	7
NA	M	2	0	2	3	2	1	6	1	7	1	4	7	5	7	5	5	7
25	F	2	0	1	2	2	2	6	1	6	1	7	7	7	7	5	7	7
31	F	2	0	2	4	6	1	6	1	6	1	6	6	7	7	6	5	6
NA	F	2	0	1	3	3	2	4	2	5	2	7	7	7	6	7	6	6
26	F	2	1	1	3	3	2	4	1	6	2	4	7	7	7	7	7	6
NA	F	2	0	1	2	2	2	6	2	6	1	7	7	7	7	6	4	7
24	M	3	0	2	2	3	1	2	2	6	1	6	7	7	5	6	6	5
NA	F	2	0	3	4	6	5	4	4	4	2	6	3	5	3	5	4	5
NA	M	3	0	2	1	3	3	5	2	7	1	6	6	7	6	7	3	7
NA	F	1	0	2	2	4	3	2	5	4	4	4	5	6	5	6	5	5
51	M	3	1	2	2	4	2	6	2	6	1	7	6	7	6	6	6	6
55	M	3	1	1	3	1	2	1	3	4	2	6	6	6	5	5	5	4
25	M	1	0	2	2	3	1	6	2	5	1	5	6	7	5	5	6	5
NA	F	2	0	2	1	5	5	6	2	5	1	4	5	7	6	7	1	5
NA	F	2	0	1	6	1	1	4	4	5	3	7	5	4	7	6	3	7
24	M	3	1	2	1	3	4	6	2	7	1	3	6	7	7	4	6	6
34	M	3	1	1	4	5	3	7	5	7	1	6	7	7	6	5	4	6
38	M	3	1	2	3	5	5	6	4	7	1	7	2	7	5	4	1	7
64	M	3	1	2	3	2	3	4	3	7	1	5	7	7	5	4	5	7
51	M	2	0	1	1	2	2	5	5	7	1	5	4	7	6	5	7	6
47	F	2	0	1	2	1	2	4	3	6	1	6	6	7	6	7	2	7
47	M	1	0	2	3	2	4	6	2	7	2	7	5	6	6	5	4	6
NA	M	2	0	1	2	4	1	6	1	6	1	6	7	7	5	6	5	6
NA	M	3	0	2	4	4	3	6	6	7	1	6	6	7	6	6	2	7
NA	M	2	0	2	2	1	2	5	7	7	2	4	5	7	6	3	4	6
NA	M	2	0	2	5	2	2	7	3	6	1	5	6	7	5	6	2	7
NA	F	2	0	1	2	1	2	1	4	7	2	6	3	6	5	4	3	7
NA	F	2	0	1	4	4	2	0	3	6	2	4	7	7	6	6	2	6
NA	F	1	0	3	3	1	3	6	3	5	1	6	5	6	5	5	5	6
NA	F	2	0	2	4	5	4	7	3	6	2	7	7	5	6	6	5	7
NA	M	2	0	1	4	3	2	3	2	7	1	6	6	6	5	7	4	6
NA	F	1	0	2	2	3	7	3	3	6	2	7	6	7	6	6	6	5

Age	Sex	Tech Exper	Had Demo	Q1	Q2	Q3	Q4	Q5	Q6	Q7	Q8	Q9	Q10	Q11	Q12	Q13	Q14	Q15
NA	M	2	0	1	2	5	3	4	3	6	2	6	6	7	6	5	3	7
NA	M	3	0	2	3	2	3	7	3	7	1	7	5	6	7	6	5	7
NA	M	2	0	2	5	1	3	5	1	7	2	4	5	7	4	4	5	5
NA	F	1	0	1	3	2	2	7	1	6	1	7	5	6	5	6	3	6
NA	M	1	0	1	3	4	4	4	1	7	1	4	7	7	3	7	5	7

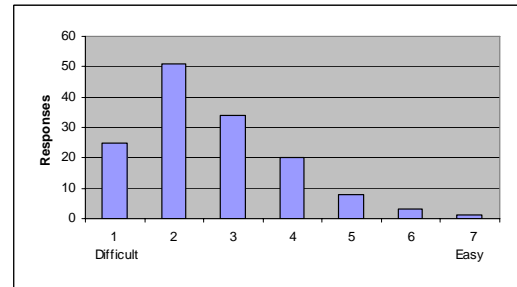
## Graphs of Phase III Survey Results

### Visual Results of Phase III Survey

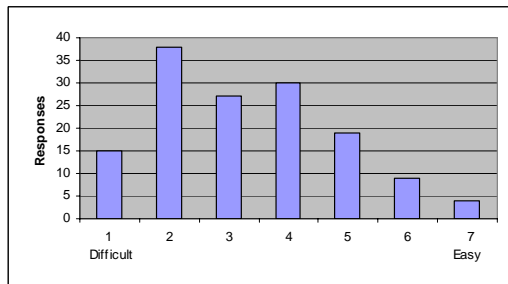
Question 1: To what degree would you consider fingerprint scanning an invasion of your personal privacy?



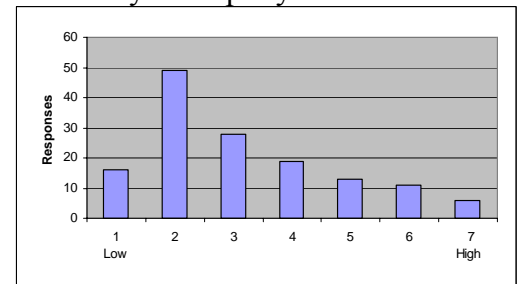
Question 2: How easy do you think it is for fingerprints to be stolen or copied?



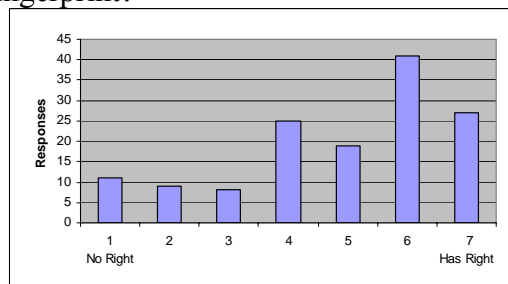
Question 3: After using a fingerprint scanner in a public setting, how easy do you think it would be for your fingerprint information to be stolen?



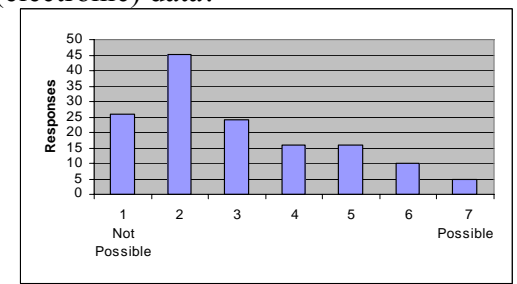
Question 4: After using a fingerprint scanner in a public setting, how concerned would you be about your fingerprint information being distributed, shared, or accessed by a 3rd party?



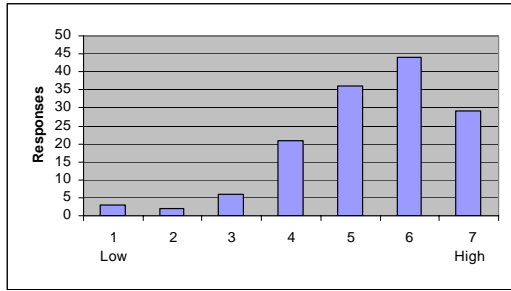
Question 5: Can any organization you work for legally require you to give your fingerprint?



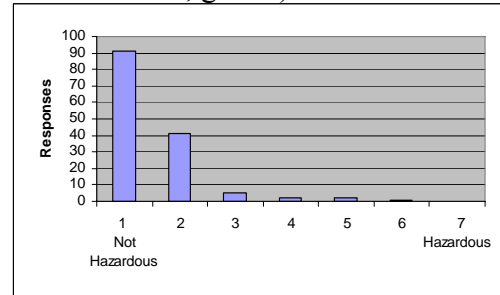
Question 6: Can a fingerprint be reconstructed from raw biometric (electronic) data?



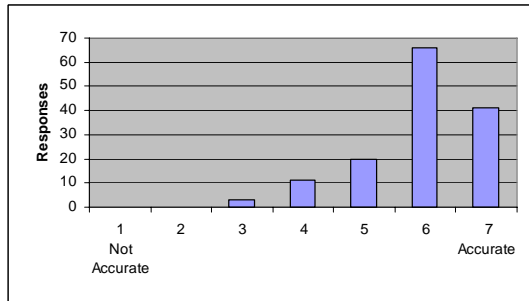
Question 7: To what degree did the previous page reassure you about fingerprint biometrics in general?



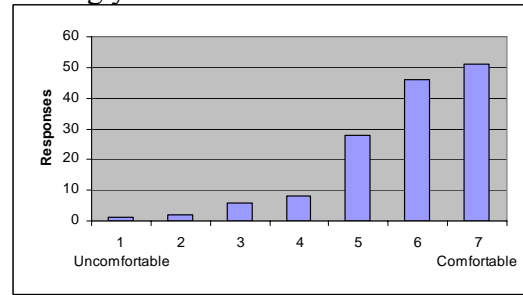
Question 8: To what degree would you consider using a fingerprint scanner hazardous to your health (i.e. pain, electrical shock, germs)?



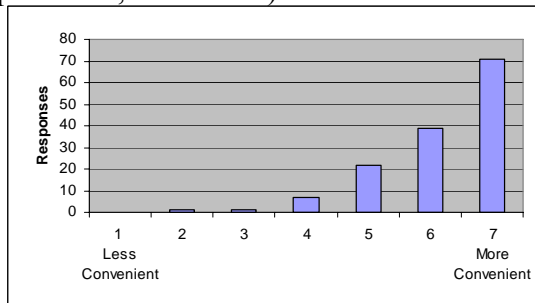
Question 9: How accurate do you think fingerprint scanners are?



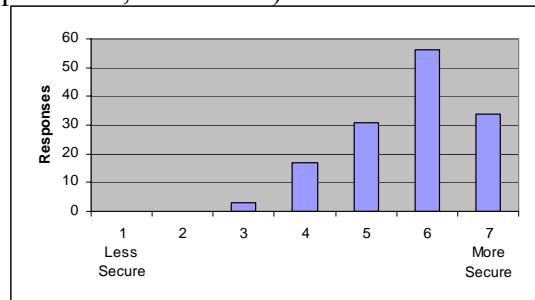
Question 10: How comfortable would you be with using your fingerprint to enter the building you work in?



Question 11: To what degree would you consider a fingerprint more convenient than other security measures (keycode, password, smart card)?

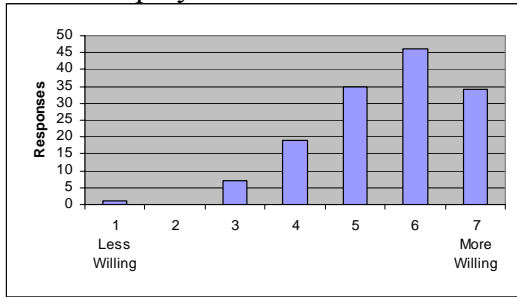


Question 12: To what degree would you consider using a fingerprint more secure than other security measures (keycode, password, smart card)?

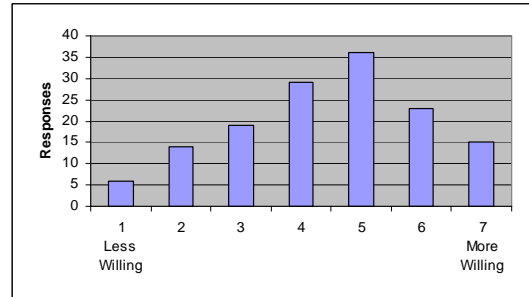




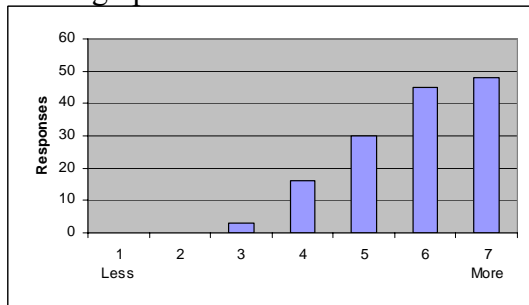
Question 13: Having read the previous information, how willing would you be to use a public fingerprint scanner at your place of employment?



Question 14: Having read the previous information, how willing would you be to use a public fingerprint scanner at a commercial location?

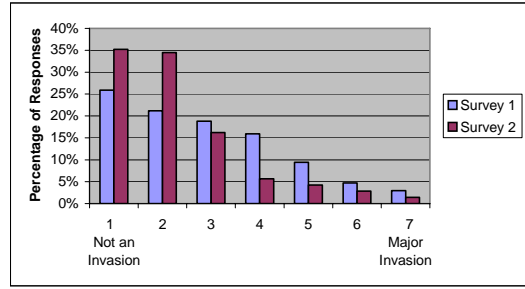
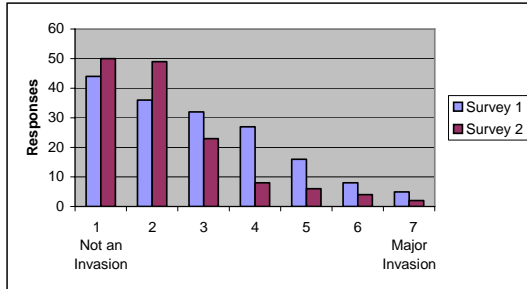


Question 15: To what degree did the previous page help you better understand how fingerprint scanners work?

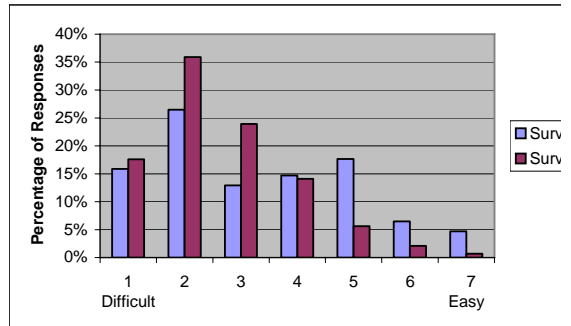
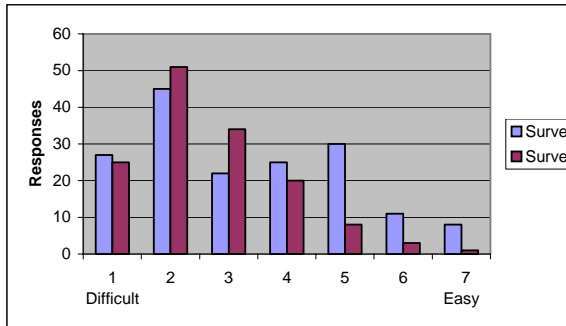


## Comparison of Phase II and Phase III Responses

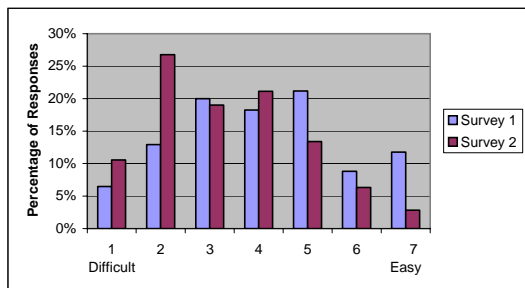
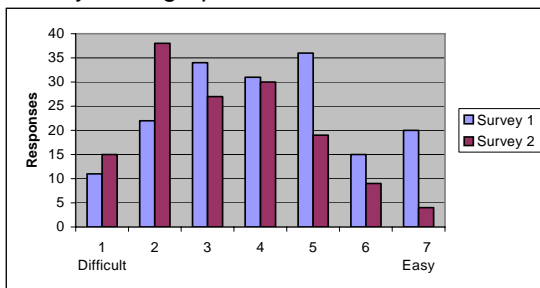
Question 1: To what degree would you consider fingerprint scanning an invasion of your personal privacy?



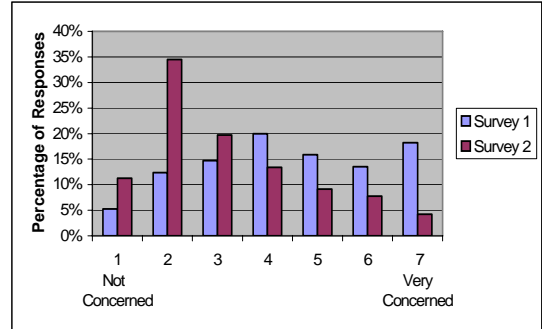
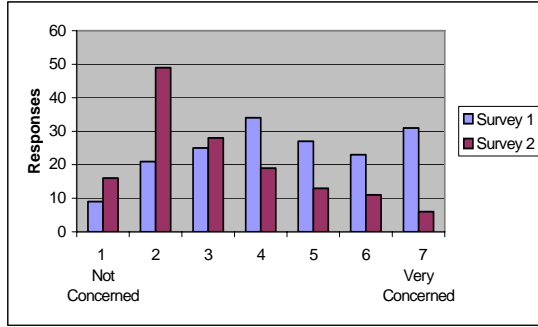
Question 2: How easy do you think it is for fingerprints to be stolen or copied?



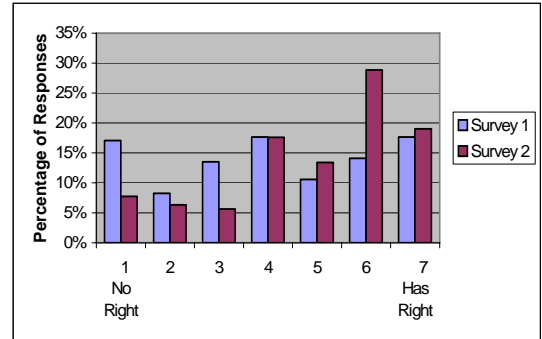
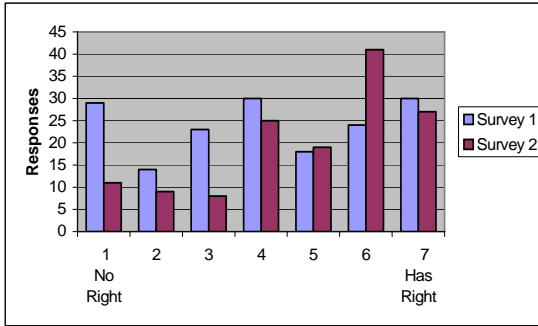
Question 3: After using a fingerprint scanner in a public setting, how easy do you think it would be for your fingerprint information to be stolen?



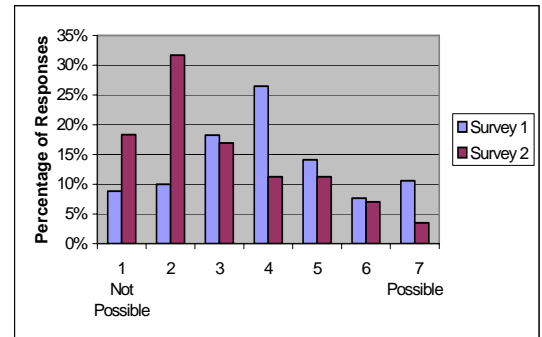
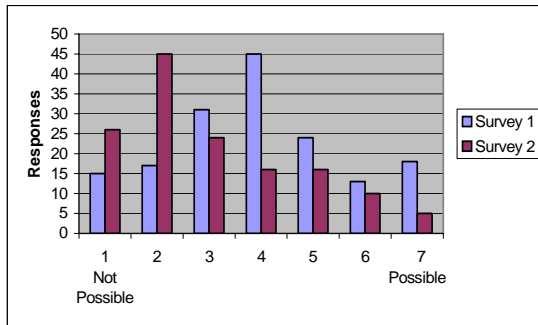
Question 4: After using a fingerprint scanner in a public setting, how concerned would you be about your fingerprint information being distributed, shared, or accessed by a 3rd party?



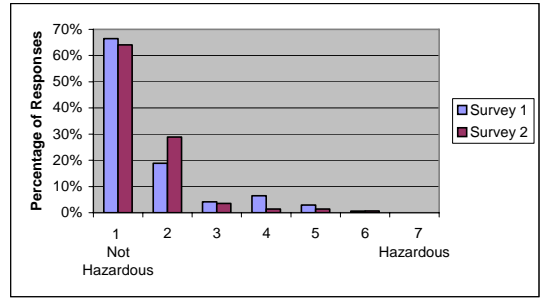
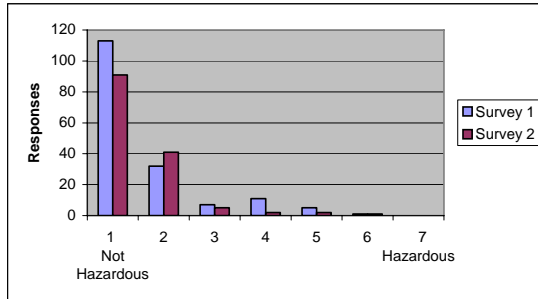
Question 5: Can any organization you work for legally require you to give your fingerprint?



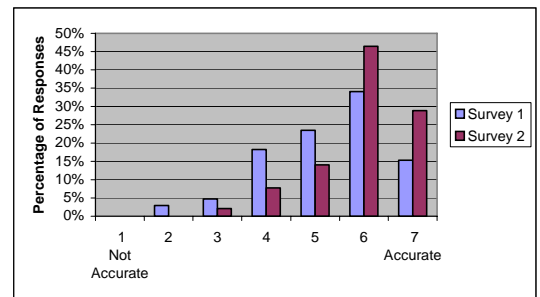
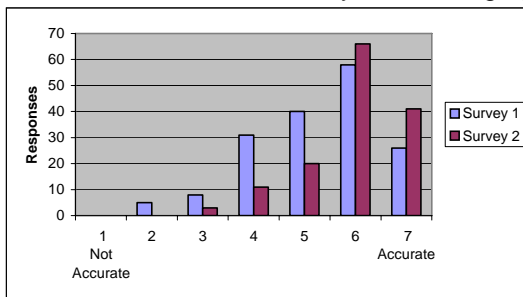
Question 6: Can a fingerprint be reconstructed from raw biometric (electronic) data?



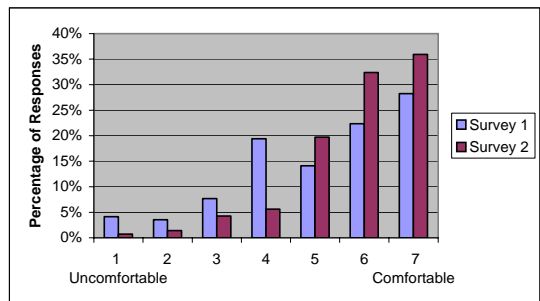
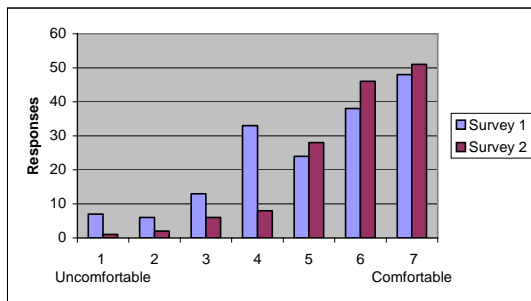
Question 8: To what degree would you consider using a fingerprint scanner hazardous to your health (i.e. pain, electrical shock, germs)?



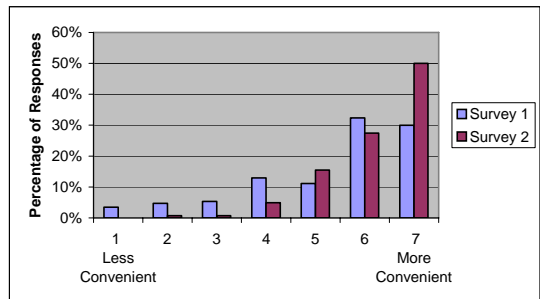
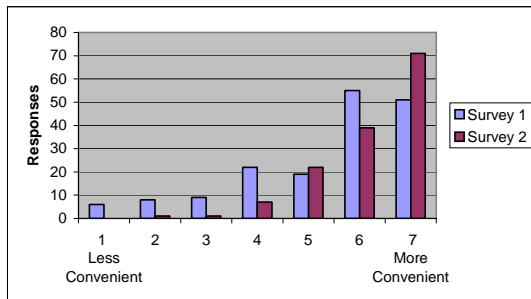
Question 9: How accurate do you think fingerprint scanners are?



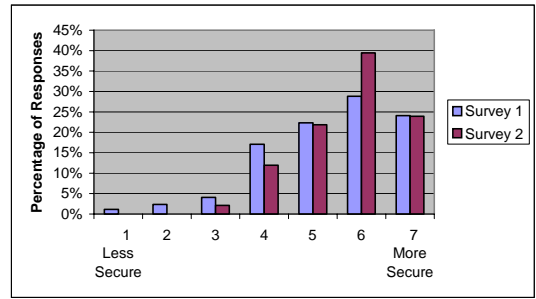
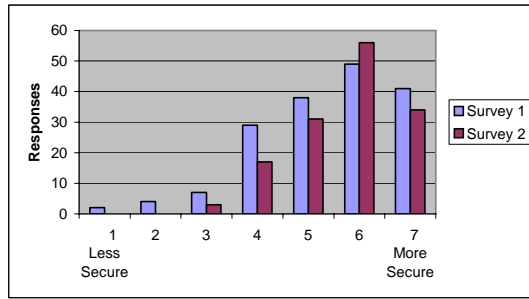
Question 10: How comfortable would you be with using your fingerprint to enter the building you work in?



Question 11: To what degree would you consider a fingerprint more convenient than other security measures(keycode, password, smart card)?



Question 12: To what degree would you consider using a fingerprint more secure than other security measures(keycode, password, smart card)?



## APPENDIX C

<b>Rep. Margaret Dayton – Voted Against</b>	
Question	Response
1	Yes. I voted no
2	Too many unanswered questions about privacy.
3	No response
4	Yes to both
5	Yes to both
6	Yes to both
7	No Response
8	Don't know

<b>Rep. Brad King – Voted For</b>	
Question	Response
1	Yes I was and I supported representative Adair on his bill.
2	I felt then and do now that the ability to have more information on the cards would be a positive thing.
3	Frankly, I thought it was killed in the house, because of some fear of personal tracking and a number of other interesting fears.
4	I think that technology exists to make the information secure.
5	Yes and yes
6	Yes and I did not get a lot of input from my constituents on it
7	I assume those same fears.
8	I believe that it was a number of ultra conservative groups
<p>(After being asked the following questions for clarification, “In response to the third question, can you elaborate about some of the 'other interesting fears' which existed about the Smart Card technology?” and “In response to the eighth question, can you tell me some of the ultra-conservative groups who opposed the legislation?”, the following response was given: “<i>You know, I really don't remember but I assume the Eagle Forum was opposed. I also believe that rep. Adair received threats over the bill</i>”.)</p>	

<b>Rep. Craig Buttars – Voted For</b>	
Question	Response
1	Yes
2	Privacy of personal information
3	Pressure from government agencies
4	Yes and yes.
5	No, more concern for government access
6	No, more concern for government access
7	Not sure
8	Not sure

<b>Rep. Wayne Harper – Voted Against</b>	
Question	Response
1	Yes. I was very involved with the sponsor, Former Rep. Gerry Adair.
2	I opposed the Smart Card and its concepts. Rep. Adair felt a Smart Card is the waive of the future and a harmless identity tool. The Smart Card is a catch all for a person's entire self. As projected to be, the Smart Card could hold all of your financial, personal, biological, medical and other private information. A card of that nature, and the corresponding information and computer system, would create a huge data base and the ability for easy identity theft. A person's ability to be unique and to go through life without being tracked becomes impossible.
3	Lack of understanding on the part of my colleagues of the need to keep personal and private information private.
4	Yes and yes. It is becoming easier every day to steal your identity and create a duplicate you. The burden is then on the victim, which takes months or years to correct the problems created by the stolen identity.
5	Yes. But also personal privacy issues were also important.
6	Yes
7	The same concerns as I raised above. Also, a number of privacy groups and information specialists were able to provide good information to the Senate so the bill would not pass.
8	Privacy, IT, and others. Also, the bill was not heard for final passage, due to the close of the legislative session.

<b>Rep. Ralph Becker – Voted For</b>	
Question	Response
1	Yes.
2	I felt the card had adequate privacy protections and had benefits to the user.
3	Don't remember
4	Privacy infringements concerns -- don't know groups.
5	Privacy infringement.
6	Had mixed response from constituents; it seemed that there were adequate protections.
7	Id theft is a big issue for me and my constituents
8	See above

<b>Rep. Sheryl Allen – Voted For</b>	
Question	Response
1	I was in Legislature when smart cards were discussed. Only minor involvement.
2	Without going back and doing research, I don't recall a House vote. It was a Rep. Gerry Adair bill so you could look that vote up if you know the year or you could look up several years under Rep. Adair's name.
3	Can't remember
4	Conservative groups in Utah went ballistic over this bill. It was considered an invasion of privacy. I do remember that Rep. Adair had to have personal protection because his life was threatened.
5	The public backlash against this bill was severe and strong. It was seen by some as "Orwellian."
6	The info could have been stolen. Since this bill was discussed, identity theft has become a major public issue. However, since this bill was discussed we've also had the 9/11 tragedy. Now I can tell you that many constituents would be willing to have an identity card that would allow them to go through airport security more quickly.
7	Opponents of this bill were passionate that the cards would be an invasion of privacy
8	No response

**Rep. Fred Hunsaker – Voted For**

Response

I was a member of the legislature from 1990 to 1997. If the Smart Card was considered by the legislature during that time, I do not remember. If I recall correctly, identify theft was not the problem then as it is now. Privacy invasion would have been a more significant issue of concern.